IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

EPIC SYSTEMS CORPORATION,

Plaintiff,

v.

TATA CONSULTANCY SERVICES LIMITED and TATA AMERICA INTERNATIONAL CORPORATION d/b/a TCA America,

Defendants.

AMENDED OPINION AND ORDER

14-cv-748-wmc

In this highly contentious lawsuit, plaintiff Epic Systems Corporation asserts a variety of federal and state law claims against defendants Tata Consultancy Services Limited and Tata America International Corporation, respectively, a much larger, India-based company and its smaller U.S. arm. Among other things, defendants provide information technology services to the U.S. healthcare industry, while Epic is a leading provider of software to this industry. Essentially, plaintiff claims that defendants accessed its web portal without authorization while servicing a mutual client, and then used information obtained to help develop their own competitive software product and for other improper purposes. Before the court are the parties' cross-motions for partial summary judgment. (Dkt. ##195, 197.)

As noted by the court in earlier opinions and explained in greater detail below, plaintiff has compelling evidence of unauthorized access by a number of defendants' employees over an extended period of time. Based on this and other undisputed evidence, the court will grant plaintiff partial summary judgment on breach of contract claims for failure to provide written notice of unauthorized access and failure to maintain

the confidentiality of Epic information and documents. The court will also grant partial summary judgment to plaintiff under the first element of the Computer Fraud and Abuse Act, 19 U.S.C. §1030(g), finding a violation of the CFAA based on defendants' unauthorized access. Finally, the court will grant plaintiff's motion with respect to its claims under the Wisconsin Computer Crimes Act, Wis. Stat. § 943.70(2)(a), based on unauthorized access and sharing of password information. In all other respects, plaintiff's motion for partial summary judgment will be denied for the reasons explained below.

In their motion, defendants correctly point out weaknesses in plaintiff's evidence of improper *use* of the accessed documents, as opposed to improper access. Nonetheless, a reasonable jury *could* find improper use based on circumstantial evidence in this record. Accordingly, the court will deny defendants' motion for partial summary judgment, save for plaintiff's conversion claim, because the property at issue is not "chattel" as a matter of Wisconsin law.[1]

[1] Also before the court is plaintiff's motion to dismiss defendants' counterclaims and to immediately sever and stay all counterclaim proceedings. (Dkt. #326.) Given that these counterclaims were only asserted late in this case, after summary judgment submissions and just a few months before trial, the court will grant the motion to sever defendants' counterclaims. The court will also address plaintiff's grounds for dismissing defendants' counterclaims in a separate opinion. All proceedings on the counterclaims are stayed until the court issues its opinion on the motion to dismiss.

UNDISPUTED FACTS[2]

A. The Parties and Key Third Parties

i. Epic

Epic Systems Corporation is a Wisconsin corporation with its headquarters in Verona, Wisconsin. Since its inception in 1979, Epic has developed, installed and supported an integrated suite of software used by hospitals, medical groups and other healthcare organizations. Epic's software is recognized in the industry as a market leader, being used by an estimated 281,000 physicians worldwide to manage the care and records of approximately 169 million patients. Epic itself now has approximately 9,500 employees located in the United States.

Epic maintains a web portal called the "UserWeb," which contains product materials, updates, training materials and other documents detailing Epic's software and its data model, as well as information on training, setup, support and operation, and details the features and configuration of Epic's software. The UserWeb also contains discussion forums where Epic customers can communicate. Epic provides access to the UserWeb to customers, who then use information from the UserWeb to install, maintain and support its software. Epic also allows third-parties (such as consultants working for customers) to access information through Epic's UserWeb web portal necessary to further implementation, integration or testing. Epic contends, however, that only a portion of the UserWeb is available to consultants working with a customer. Furthermore, it

[2] Unless otherwise noted, the court finds the following facts material and undisputed when viewed in a light most favorable to the non-moving party on that particular issue.

appears that consultants generally need to sign a UserWeb Access Agreement that expressly restricts their use of this information.

The parties dispute whether Epic takes sufficient precautions to protect access to the UserWeb, including how Epic authorizes individual registration of UserWeb accounts. Because these facts are marginally relevant to the issues before the court on summary judgment, these factual disputes are not recounted except where germane to the specific issue being discussed in the opinion below. (*See* Defs.' PFOFs (dkt. #210) ¶¶ 23, 82-92; Pl.'s Resp. to Defs.' PFOFs (dkt. #417) ¶¶ 23, 82-92; Pl.'s Add'l PFOFs (dkt. #415) ¶¶ 583-87.)

ii. TCS

Defendant Tata Consultancy Services Limited ("TCS India") is an Indian corporation that provides information technology services, consulting and business solutions on a global scale, and offers a wide portfolio of infrastructure, engineering and assurance services. TCS India is part of the Tata Group. TCS India has more than 318,000 employees in 42 countries.

Defendant TCS America International Corporation ("TCS America") is a New York corporation, wholly owned by TCS India. Plaintiff presents evidence that TCS America is simply the U.S. arm of TCS India, including the testimony of defendants' corporate representative, Syama Sundar, that (1) defendants do not "distinguish" between TCS America and TCS India and (2) the two entities are considered "one and the same." (Pls.' PFOFs (dkt. #213) ¶¶ 49-61.) Defendants do not dispute the specific facts proposed by plaintiff, but dispute that "there is any evidence that TCS India and

TCS America were the agents of each other at the times mentioned" in the complaint. (*See, e.g.*, Defs.' Resp. to Pl.'s PFOFs (dkt. #308) ¶ 58.) The court need not resolve this agency issue either. Instead, the court will at times simply refer to defendants jointly as "TCS," consistent with the parties' treatment.

Although TCS's number one source of revenue is work done in the United States, which accounts for 56% of total revenue, it appears that TCS has only recently begin to penetrate the market for healthcare software. TCS's software product, Med Mantra, is a consolidated, comprehensive, integrated hospital management system. TCS began development of Med Mantra's predecessor, EHIS, in 2006. Med Mantra has been implemented at 17 hospitals and 44 clinics, all part of the Apollo Group in India and the Cancer Institute in Adyar, Chennai.[3] Defendants contend that the development of Med Mantra has been driven by Apollo and that it is not a good fit for other Indian hospitals. Still, as plaintiff points out, some marketing materials describe Med Mantra's vision "to be recognized as a world leading Health Care Provider solution." (Pl.'s PFOFs (dkt. #213) ¶ 45 (quoting Richmond Decl., Ex. 12 (dkt. #227-1) 26.) Defendants nevertheless claim that Med Mantra is an Indian solution and not something TCS planned to implement worldwide, at least in the short term.[4] (*See* Defs.' Resp. to Pl.'s Add'l PFOFs (dkt. #460) ¶ 562.)

[3] At some point, TCS removed Apollo-hospital specific functionality and branded a product called TCS Hospital Information Exchange "TCS-HIS."

[4] As described in more detail below, TCS also developed a software product in 2014 for a hospital located in Colorado, DaVita Kidney Care. (Pl.'s Resp. to Defs.' PFOFs (dkt. #417) ¶ 161; *see also infra* Facts § C.iii.b.)

iii. Kaiser Permanente

While not a party to this action, Kaiser Permanente figures prominently in the parties' dispute. Kaiser Permanente, sometimes referred to as "KP," is a not-for-profit healthcare organization with approximately 150,000 employees who provide care to approximately 8.7 million members. Kaiser Permanente is the largest managed healthcare organization in the United States. Kaiser Permanente consists of Kaiser Foundation Health Plan, Kaiser Foundation Hospitals and their subsidiaries, and the Permanente Medical Groups. Kaiser Foundation Hospitals ("Kaiser") operates a chain of medical centers, hospitals, medical offices and clinics, primarily on the West Coast of the United States.

iv. Philippe Guionnet

Because his role is central to the development of plaintiff's claims, the court will introduce one more key player to this dispute upfront. In October 2012, TCS hired Philippe Guionnet as the vendor engagement executive for the Kaiser account. TCS's CEO Natarajan Chandrasekaran (commonly referred to as "Chandra") recommended Guionnet to Sundar, the head of the Kaiser account at that time. Before his employment with TCS, Guionnet worked as a Chief Information Officer at Cendant and Avis, a Deputy Chief Information Officer at Disneyland Paris and a national Director of KPMG.[5] As will be described below in more detail, Guionnet was the individual who

[5] Defendants propose several facts concerning Guionnet's email campaigns, dating back to 2013, in which he sought a promotion and increased responsibilities. (Defs.' Add'l PFOFs (dkt. #300) ¶¶ 1-2, 4-6, 8-9.) While these facts may go to Guionnet's credibility, the court does not make credibility assessments at summary judgment, and therefore has not considered these facts and will not describe them in further detail in this opinion.

informed the parties and Kaiser of his suspicion that TCS was accessing Epic's UserWeb without authorization and improperly using documents from the UserWeb.

B. Epic, Kaiser and TCS's Business Relationship

i. Epic licenses software to Kaiser

On February 4, 2003, Epic entered into a written agreement with Kaiser to license computer software to Kaiser. Kaiser uses Epic's software as an electronic health record ("EHR") that gathers and utilizes patient information. Kaiser refers to specific Epic modules it uses at KPHealthConnect. As an Epic customer, Kaiser has access to the UserWeb.

Pursuant to the terms of their agreement, Kaiser is accountable to Epic for inappropriately sharing Epic's intellectual property with third parties, but that agreement does not require Kaiser to ensure that those third parties enter into a separate contract directly with Epic.

ii. Epic enters into 2005 Agreement with TCS

TCS began working with Kaiser in 2005. In early August of 2005, Epic learned that four individuals from TCS had registered for some classes at Epic. Originally, Epic thought that the individuals attempting to attend Epic classes were Kaiser employees. When Epic learned that the individuals were actually TCS employees, it asked Kaiser for more details about TCS's role with Kaiser. Upon learning that Epic did not have a non-disclosure agreement with TCS, Epic removed the individuals from the class and required that they leave their materials behind. Epic later explained in an email to a contact at Kaiser that Epic was being "extra vigilant" because, in the past, "a student [had]

claim[ed] to be from [Kaiser] but was actually from a competitor." (Pl.'s PFOFs (dkt. #213) ¶ 90 (quoting Richmond Decl., Ex. 19 (dkt. #230-1) 4).)

In response to this episode, Epic and TCS America entered into a Standard Consultant Agreement ("the Agreement" or "the 2005 Agreement"), dated August 10, 2005, and signed by Satya Hedge, senior vice president and general counsel of TCS India. (Richmond Decl., Ex. 20 (dkt. #230-2).) The Agreement states that its "validity, construction and enforcement . . . shall be determined in accordance with the laws of Wisconsin, without reference to its conflicts of laws principles." (*Id.* at 4.)

Among other provisions, the Agreement contains a section titled "CONFIDENTIALITY AND USE RESTRICTIONS." (*Id.* at 2-3.) As part of that section, TCS agreed that "Epic's Program Property contains trade secrets of Epic protected by operation of law and this Agreement." (*Id.* at 2.) The Agreement further contains several obligations for TCS, including:

- "Maintain in confidence any Confidential Information, except that [TCS] may disclose Confidential Information relating to the Program Property to Epic's licensees to the extent necessary for such licensees' implementation of the Program Property, with the understanding that such information shall be kept confidential by the licensees under their respective license agreements with Epic;"
- "Use any Confidential Information only for the purpose of implementing the Program Property on an Epic customer's behalf;"
- "Limit access to the Program Property to those of [TCS's] employees who must have access to the Program Property in order to implement the Program Property on Epic's or its customer's behalf;"
- "Store all copies of the Program Property in a secure place;"
- "Notify Epic promptly and fully in writing of any person, corporation or other entity that [TCS] know[s] has copied or obtained possession of or access to any of the Program Property without authorization from Epic;" and

- "Not permit any employee while in [TCS's] employment who has had access to the Program Property or any Confidential Information relating to the Program Property to participate in any development, enhancement or design of, or to consult, directly or indirectly, with any person concerning any development, enhancement or design of, any software that competes with or is being developed to compete with the Epic Program Property for a period of at least two (2) years after the date that such employee last has access to such Program Property or Confidential Information."

(*Id.* at 2-3.)

"Confidential Information" is defined as

> Any information [TCS] employees obtain from Epic or any Epic licensee as to the Program Property, Epic or Epic's plans or customers, including without limitation information concerning the functioning, operation or Code of the Program Property, Epic's training or implementation methodologies or procedures, or Epic's planned products or services, but excluding any information that: (a) is now or hereafter becomes publicly known through no act or failure on the part of [TCS] and without breach of the Agreement; (b) is known by [TCS] on a nonconfidential basis at the time of the receipt of such information from Epic or an Epic licensee, or (c) subsequently becomes known by [TCS] on a non-confidential basis, or (d) developed by [TCS] independently without use of or reliance on Confidential Information.

(*Id.*) The Agreement defines "Program Property" as "the computer program object and source code and the Documentation for all of Epic's computer programs." (*Id.* at 2.) "Documentation" is defined as "any instructions, manuals or other materials created by Epic in any format, relating to the implementation, operation or Code of the Program Property." (*Id.*) "Code" is defined as "both the object and source code of the Program Property."

The Agreement also provides in relevant part that:

> No notice required to be provided shall be effective unless it is in writing; is delivered to the other party by either reputable overnight courier, U.S. mail by registered, certified,

> or overnight delivery special, with all postage prepaid and return receipt requested, or by personal delivery; and is addressed to:
>
> If to Epic:
>
> Judith R. Faulkner, CEO
> Epic Systems Corporation
> 5301 Tokay Boulevard Madison, WI 53711

(*Id.* at 3-4.)

This Agreement was in effect between TCS America and Epic for the time period relevant to plaintiff's claims. Epic terminated the Agreement on October 30, 2014, shortly after it filed this lawsuit. The parties agree that the Agreement is enforceable and unambiguous; they also agree it was not modified. Furthermore, TCS does not contend that its performance under the contract was somehow excused.

iii. Kaiser engages TCS to test software

In 2011, Kaiser engaged TCS to test Epic software in its so-called "Testing Center of Excellence" ("TCoE"). The TCoE work included providing testing support for regularly-scheduled Epic releases, major upgrades, steady state maintenance testing and new investment projects. Approximately 1,000 TCS employees were devoted to the Kaiser account, and "a lot more people" were partially involved with that account. (Pl.'s PFOFs (dkt. #213) ¶ 134.) Defendants do not dispute these numbers, but contends that not all of these individuals were involved with Epic software. Also, employees were located both "offshore" in India and "onshore" at Kaiser facilities in the United States.

The relationship between TCS America and Kaiser was governed by their Amended and Restated Masters Services Agreement ("MSA"), dated January 29, 2012.

(Richmond Decl., Ex. 29 (dkt. #231).) TCS India and TCS America are also parties to their own "back-to-back agreement," which in turn governed their work pursuant to the MSA with Kaiser. While the MSA provides an "umbrella framework," individual pieces of work are executed in statements of work or work orders, sometimes referred to as "SOWs." (Pl.'s PFOFs (dkt. #213) ¶ 143 (quoting Sundar Depo. (dkt. #125) 65).)

The MSA required TCS America and TCS India to perform services at approved facilities, referred to as Offshore Development Centers ("ODCs"), and specifically identified the facilities located at "Chennai and Kolkat[]a, India." (Pl.'s PFOFs (dkt. #213) ¶¶ 150-55.)[6] The ODCs were to be used for Kaiser work only. Only employees who work at the ODC or have a reason to be there are allowed to enter the building. All TCS employees entering the ODC had to pass through security using a badge.

To protect its own confidential information, Kaiser also required that security protocols be implemented in the ODCs, including that: (1) antivirus software had to be up-to-date; (2) any printing had to be on colored paper and shredded after use; (3) CD drives and USB ports had to be disabled to insure that TCS employees could not copy data; (4) access to the TCS email system was prohibited; (5) TCS employees were not allowed to use their phones; and (6) with the exception of lead managers, TCS employees were prohibited from sending emails from Kaiser email addresses to non-Kaiser email

[6] In other parts of the record, it appears that another approved ODC is located in Hyderabad. (*See* Defs.' PFOFs (dkt. #210) ¶ 46.) Regardless, there is no dispute that all of the offshore development centers were located in India.

addresses. In the ODCs, TCS employees were also provided computers that could only connect to the Kaiser network.[7]

Under the MSA, TCS employees also were not to use Kaiser's software except as expressly permitted. This included software Kaiser licensed from some third party, which in turn included Epic's software. In addition, there was a policy against using other people's log-on and password information.

Kaiser's security policies were posted at every desk in the ODC, and TCS claims that the importance of information security was continuously communicated to the Kaiser team. In particular, TCS claims that it hosted multiple security awareness sessions where employees were reminded not to share passwords or otherwise compromise client confidential information. (*See also* Pl.'s Add'l PFOFs (dkt. #415) ¶¶ 570-77, 652-56.) The TATA Code of Conduct, which governs the behavior of TCS employees, also states that "[a]ny collection of competitive information shall be made only in the normal course of business and shall be obtained only through legally permitted sources and means." (Pl.'s PFOFs (dkt. #213) (quoting Richmond Decl., Ex. 34 (dkt. #232-2) 3.)

Despite these security provisions, TCS provided separate computers (referred to as "kiosk machines") in the ODC that *could* be used to access the internet, TCS's network and TCS email. Additionally, there were computers outside of the ODC, but in the same building, that could be used to access TCS email and the internet. Defendants maintain that these computers did not have internet access and that the USB ports were disabled, but Epic points out that the deposition testimony on which defendants rely is

[7] At least some TCS employees were issued Kaiser email addresses using the "kp.org" domain.

contradicted by other testimony from the same witness that he *did* use those computers to access the internet. Moreover, defendants' Head of Information Security for Insurance and Healthcare admitted in an external audit that the USB ports were not disabled.

iv. TCS attempts to partner with Epic

In May 2011, a delegation of TCS and Kaiser executives visited Epic's headquarters in Wisconsin. During the meeting TCS presented a deck of slides explaining its business, among other things. The presentation revealed that TCS had developed medical software (Med Mantra) for use at the Apollo Hospital in India. After review of TCS's website, Epic's leadership -- particularly, its President Carl Dvorak -- was concerned that TCS had not been forthright about their development of Med Mantra and decided not to work with TCS.[8]

Still, the parties' mutual customer, Kaiser, continued to push for Epic to work with TCS. Suresh Muthuswami, TCS's President of Insurance & Healthcare Business Group, also continued to reach out to Dvorak on several subsequent occasions. During the course of these communications, Muthuswami attempted to ease Epic's concern that "confidential information might somehow find its way to the Med Mantra team" by offering to bring over a TCS expert in Med Mantra to speak with Epic and otherwise ensure that the "unit at TCS that would do Epic work" would remain separate from the unit working on Med Mantra. (Pl.'s PFOFs (dkt. #213) ¶ 212 (quoting Muthuswami

[8] At that time, Epic generally refused access to Indian firms based on a concern that "such firms may lack the technical aptitude and willingness to prevent leaks and the difficulty of pursuing legal recourse in a foreign country." (Pl.'s Resp. to Defs.' PFOFs (dkt. #458) 417) ¶ 70.)

Depo. (dkt. #158) 62-63); Defs.' PFOFs (dkt. #210) ¶ 73 (quoting Dvorak Depo. (dkt. #187) 101).) Despite Kaiser's assurance that TCS "will sign anything," Dvorak continued to express concerns about TCS to his contact at Kaiser, explaining that TCS may have a "competitive interest." (Pl.'s PFOFs (dkt. #213) ¶ 213-14 (quoting Richmond Decl., Ex. 38 (dkt. #232-6); Defs.' PFOFs (dkt. #210) ¶ 75 (quoting Robben Decl., Ex. 14 (dkt. #204-14)).)

In 2012, TCS again sought multiple times to build a partnership with Epic, attempting to set up a face-to-face conversation.[9] Again, Dvorak expressed concerns to his contact at Kaiser that "the situation with TCS was a 'deeper competitive situation than initially understood.'" (Pl.'s PFOFs (dkt. #213) ¶ 218 (quoting Richmond Decl., Ex. 39 (dkt. #232-7)).) Around this same time, Dvorak also exchanged emails with TCS's Muthuswami, stating that "details relating to competitive activity by Tata" is an "ongoing and key problem," and "[i]f you are truly a competitor, it may well be that there is no framework that would be possible." (Pl.'s PFOFs (dkt. #213) ¶¶ 219-20 (quoting Richmond Decl., Ex. 40 (dkt. #232-8).) In discussions regarding TCS access to Epic's UserWeb, Epic also wanted to "understand specifically what documents [TCS] need[ed] and what their job functions [were] going to be" before granting access. (Pl.'s PFOFs (dkt. #213) ¶ 205 (quoting Rehm Depo. (dkt. #185) 36-37, 42-43).)

Despite all of these efforts, TCS could not reach an agreement with Epic. Therefore, no TCS associate was allowed to connect directly to the UserWeb. TCS

[9] Around this same time, a TCS employee Arun Agarwal emailed Muthuswami that: "There was one guy in our team who had access to EPIC. He left us recently. Now we have no one. Dire State. Need to have Carl give us access to EPIC at least in KP." (Pl.'s Add'l PFOFs (dkt. #460) ¶ 590 (quoting Saros Decl., Ex. 1 (dkt. #258-1)).)

acknowledged this restriction on its access to the UserWeb at depositions during this lawsuit, as well as in earlier, contemporaneous presentations. (*See* Pl.'s PFOFs (dkt. #213) ¶¶ 224-26 ("TCS is not an Epic partner. As a result, they are not allowed to access Epic Systems UserWeb portal.") (quoting Medikondra Depo. (dkt. #161) 196-97; Richmond Decl., Ex. 42 (dkt. #233) p.4.).) At summary judgment, TCS does not appear to dispute this restriction either, although it states generally and without explanation that access was somehow permitted under the 2005 Agreement. (Defs.' Resp. to Pl.'s PFOFs (dkt. #308) ¶ 227.)

v. TCS creates "workaround"

Faced with this obstacle, TCS employees devised a "workaround" to obtain information needed from Epic without accessing the UserWeb, including the information required to create "test scripts." Under the workaround, Kaiser employees would download release notes from the UserWeb for TCS employees to access. These release notes were to be held in a repository at Kaiser. Defendants' corporate representative, Syama Sundar, testified at his deposition that there should not be "any Epic documentation at TCS" because everything is "within Kaiser," and there was "no reason whatsoever" that "TCS employees needed to go to Epic's UserWeb." (Pl.'s PFOFs (dkt. #213) ¶¶ 233, 236 (quoting Sundar Depo. (dkt. #) 415-16.) Still, two TCS employees who figure prominently in this case, Ramesh Gajaram and Aswin Anandhan, explained at their depositions that there were times when relying on either Epic or Kaiser personnel to obtain information took time.

In addition, Anandhan would contact an Epic employee, Michael Buchanan, who sent Anandhan documents from time to time, including information that was similar to that available on the UserWeb. Buchanan also would host WebEx sessions where he would share his screen with Anandhan.

C. TCS Accesses Epic's UserWeb

i. Gajaram shares UserWeb credentials

At some point, work on the Kaiser account was transferred from TCS to another company, Computer Sciences Corporation ("CSC"), headquartered in Virginia, and later back again to TCS. In particular, a CSC engineer from India, Ramesh Gajaram, began working on the Kaiser account in February 2006. During this time, Gajaram was given a Kaiser email address. In January 2011, Gajaram also registered and was given access to Epic's UserWeb. In his application for a UserWeb account, Epic represents that Gajaram did *not* identify that he was a consultant rather than a Kaiser employee.

After a Kaiser employee recommended TCS hire Gajaram, Gajaram left his job at CSC and started work at TCS.[10] From September 2011 until March 2014, Gajaram then

[10] Relying on testimony from whistleblower Phillipe Guionnet, Epic contends that TCS hired Gajaram *because* of his UserWeb account. TCS contends that there was no discussion of Gajaram's UserWeb account during the hiring process, and TCS was not aware that Gajaram had access at that time. There is, however, evidence to support Guionnet's belief: namely, defendants knew Gajaram was conducting testing during his employment at CSC; defendants trained Gajaram on how to use Epic's system during his employment at CSC; and Gajaram shared his credentials immediately following his joining TCS. (Pl.'s Resp. to Defs.' PFOFs (dkt. #417) ¶ 100.) Because this allegation does not appear central to plaintiff's fraud claim, the court need not sort through this dispute, other than to note that Gajaram was also hired during the thick of TCS's efforts to develop a partnership agreement with Epic to allow access to the UserWeb. While none of these facts constitute a "smoking gun," they create enough smoke for a reasonable jury to infer a gun may be in there somewhere. Of course, even that merely permits an inference that Gajaram was attractive to TCS for his general knowledge of Epic software, and perhaps special access, not that defendants intended to use it for an improper purpose.

worked in Chennai, India, on TCS's Kaiser account as part of the Testing Center of Excellence. During this time period, his job consisted of testing Epic products for use at Kaiser. In addition, Gajaram served as an Information Security Coordinator, which involved monitoring TCS's and Kaiser's security protocols to protect Kaiser's and Epic's confidential information.

Despite TCS's workaround, Gajaram believed he still needed direct access to the UserWeb. In particular, Gajaram testified that he believed lack of access to the UserWeb would delay his team's work. The UserWeb Access Agreement states that if a user is "granted UserWeb access," he or she "agree[s] not to access the UserWeb outside the U.S. and Canada without prior express written consent from Epic." (Pl.'s Add'l PFOFs (dkt. #415) ¶ 556 (quoting Richmond Decl., Ex. 44 (dkt. #233-2)).)[11] Nevertheless, Gajaram continued to use his Kaiser credentials after leaving CSC's employ to access and download documents on the UserWeb while employed by TCS in Chennai, India.

Initially, Gajaram used his Kaiser-issued computer to access Epic's UserWeb. After a brief period of time, however, Kaiser blocked his access. Gajaram then used the TCS kiosk computers to access the UserWeb, viewing and downloading documents to the kiosk's hard drive and then emailing them from his tcs.com email address to his kp.org email address.

Soon after he started working at TCS in the fall of 2011, Gajaram's manager and the program manager for TCoE, Mukesh Kumar, learned that Gajaram had access to

[11] The record does not indicate whether Gajaram signed the UserWeb Access Agreement, either physically or electronically, but there appears to be no dispute that he was bound by its terms.

Epic's UserWeb. In late 2011 and early 2012, Kumar specifically asked Gajaram to log into the UserWeb so that he could see what it looked like. Gajaram estimates that Kumar and he had around ten other conversations about the UserWeb. At his deposition, Gajaram testified that he shared his credentials with three other TCS employees as well -- Sankari Gunasekaran, Aswin Anandhan and Muriagh Manikandan.[12] These employees in turn also accessed the UserWeb and downloaded documents from it.

In addition, other TCS employees had access to Epic's UserWeb, including at least Nazia Khader, Abhisek Bhowmik, Brindha Saiprasad, Revathi Puroshotham, Tapas Mondal, Saswat Mishra, Agnihotra Ghosh, Gautam Chhibber, Deepa Pandurangan, Apurva Dwivedi, Ms. Manjusha, and Ms. Madhavi.[13] (*See also* Pl.'s Add'l PFOFs (dkt. #415) ¶¶ 614, 623-32 (detailing information from January 2016 depositions of TCS employees who accessed the UserWeb using Gajaram's credentials).) Gajaram further testified that Kumar was aware that he had shared his login credentials with other TCS employees.

For his part, Anandhan testified that he would download documents from the UserWeb, email them from his TCS email address to his Kaiser email address or to other team members, as well as download some or all of them to the TCS "knowledge

[12] While TCS points out that Manikandan denies ever receiving a UserWeb password (Defs.' Resp. to Pl.'s PFOFs (dkt. #308) ¶ 295), that is obviously a credibility issue for the jury.

[13] The parties dispute the exact number of TCS employees who accessed the UserWeb. Epic represents that 29 people accessed it. TCS contends that the number is far fewer, representing that four individuals downloaded documents and that another nine individuals accessed the UserWeb but deny downloading anything. (Pl.'s Resp. to Defs.' PFOFs (dkt. #417) ¶ 126; Defs.' Reply to Defs.' PFOFs (dkt. #458) ¶ 126.) While the exact number of individuals is not critical to any of plaintiffs' claims, to the extent that TCS has failed to discover the exact number based on the inadequacy of its investigative efforts, that fact may be material to plaintiff's claims.

repository," where his ten-member team could access them. In addition, Anandhan shared Gajaram's credentials with most, if not all, of his team, including some of the individuals included in the list above.

In May 2012, Anandhan left Chennai and began working in Pleasanton, California, where he remained until February 2015. During that period, his offshore team continued to use Gajaram's credentials. In January 2012, Anandhan applied for his own UserWeb credentials. In his application, Anandhan stated that he lived in Pasadena, California, despite his not living in the United States at that time and *never* residing in Pasadena. Anandhan's request was denied.

Approximately 15 months after Gajaram changed employment from CSC to TCS, on or about December 3, 2012, he finally updated his UserWeb registration to inform Epic that he was now an employee of TCS working for Kaiser. Epic sent no response to Gajaram's update, much less one stating that he should no longer have access to its UserWeb, although an Epic employee testified at his deposition that Epic *intended* to deactivate Gajaram's account. Instead, the account was apparently mistakenly marked as "expired," which allowed Gajaram to click on a link and reactivate his account. (Pl.'s Resp. to Defs.' PFOFs (dkt. #381) ¶ 41 (quoting Rehm Depo. (dkt. #185) 146-48).) As a result, Gajaram continued to use his UserWeb account in 2013 and 2014. During this period, he also renewed his account every 120 days as required, and in doing so, reaffirmed each time that he was a TCS consultant for Kaiser.[14]

[14] Plaintiff represents in its opposition to defendants' motion for summary judgment that Gajaram had already renewed his account on three occasions after joining TCS before disclosing in December 2012 that he was employed by TCS, the implication being that Gajaram mislead

In March 2014, Gajaram moved to Portland, Oregon, where he worked as TCS's Onshore Test Lead or Onshore QA Lead. On March 26, 2014, Gajaram emailed Ranjeet Kumar, a CSC (rather than a TCS) employee, an attachment entitled "AMB100_EpicCar_Ambulatory_Fundamentals_TC.zip," which contained a group of documents from Epic's UserWeb. (Pl.'s PFOFs (dkt. #213) ¶ 351; Richmond Decl., Ex. 60 (dkt. #234-3).) At the time he sent Kumar these documents, Gajaram testified that they were both working on the Kaiser project. Gajaram further testified that Kumar, like Gajaram, was working on testing or implementing Epic software and wanted to understand the workflow of the ambulatory modules.

In April 2014, Gajaram told Anandhan that he had changed his UserWeb password, and then shared the new password with him, while telling him not to communicate it to other members of his offshore team. Gajaram testified that Anmol Gupta, a TCS engagement manager responsible for heading up the TCoE, assured Gajaram that he could share his new password with Anandhan, but not others. At the direction of Gupta, Anandhan also created another UserWeb account under the name of another of his team members, Deepa Pandurangan.[15]

Epic in each of those earlier renewals. (Pl.'s Opp'n (dkt. #414) 14 (citing Pl.'s Add'l PFOFs (dkt. #415) 563).) There is no direct support for either this representation or the implication. Indeed, plaintiff merely cites to testimony of one of its employees as to when Gajaram first updated his registration to disclose he was a consultant with TCS. (Rehm Depo. (dkt. #185) 138-40.) At best, plaintiff seems to infer from the requirement of 120 day updates *after* his initial disclosure, that he had a similar obligation before.

[15] Despite this, Pandurangan testified at her deposition that Anandhan later told her to tell TCS investigators that she mistakenly created her own UserWeb account, rather than the truth.

In May 2014, yet another TCS employee Muriagh Manikandan, emailed Gajaram and asked him for his UserWeb login credentials. In June 2014, Gajaram emailed another TCS employee Priya Ramamoorthy asking her to access the UserWeb -- since TCS was not allowed to use the UserWeb from offshore -- and "share with us additional details." (Pl.'s PFOFs (dkt. #213) ¶ 281 (quoting Richmond Decl., Ex. 53 (dkt. #233-11)).) Again, in June 2014, Ramamoorthy and Gajaram exchanged emails about Gajaram's access to the UserWeb.

On June 24, 2014, Manikandan informed Gajaram that Epic had blocked access to the UserWeb using Gajaram's credentials. After confirming with Anandhan that he, too, could not access the UserWeb with his credentials, Gajaram emailed userwebaccount@epic.com, informing Epic that he could not log in and asking them to re-enable his account. Gajaram provided his name, user ID, and his Kaiser email address. Two days later, Gajaram sent another email to the same address, forwarding his prior email. On June 30, 2014, Gajaram sent another email asking for an update.

In his June 30, 2014, email, however, Gajaram's signature block had been changed to remove any reference to "TATA Consultancy Services," instead just listing "Kaiser Permanente." Plaintiff argues that these changes were intentionally deceptive, although TCS challenges this based on Gajaram already having informed Epic in December 2012 that he was an employee of TCS working for Kaiser.

Gajaram now acknowledges that "ethically speaking," he should not have shared his login credentials. (Pl.'s PFOFs (dkt. #213) ¶ 268 (quoting Gajaram Depo. (dkt. 128) 163).) TCS also acknowledges that it was an "industry standard policy" that "people

should not be sharing their access credentials with other people." (Pl.'s PFOFs (dkt. #213) ¶ 241 (quoting Muthuswami 30(b)(6) Depo. (dkt. #188) 60).) Even after Gajaram's account was closed, TCS employees continued to use Pandurangan's credentials to access the UserWeb.

ii. TCS employees download and share Epic documents from UserWeb

From June 2012 to June 2014, individuals using Gajaram's UserWeb credentials downloaded over 6,000 documents and more than 1,600 unique files. Epic's designated expert Stirling Martin, a senior vice president and the interim chief security officer for Epic, opines that the downloaded documents "contain detailed information on the features and functionalities of Epic's software and database systems developed over thirty years." (Decl. of Stirling Martin (dkt. #8) ¶ 11.) Epic's expert further opines that the documents:

- include information that is highly sensitive to Epic and would allow a competitor to reverse engineer the functionality of Epic;
- describe programming approaches and processes developed to produce optimal functionality of Epic's software;
- provide detailed data model and source code information; [and]
- detail the system capabilities and functions of Epic's software, such as procedures for transferring data, rules related to information collection, methods for limiting access to patient records and data, and processes for converting customer data.

(*Id.* at ¶ 11.)[16] From all of this, Stirling concludes that the documents would "enable the holder to short-cut years of development and investment" and provide a competitor with

[16] Pertinent to Epic's Wisconsin's Uniform Trade Secrets Act claim, Epic also claims that 36 files constitute trade secrets. Defendants contend that the 36 documents are "in fact User Guides or

> a drastic competitive advantage because it will be able to develop a competing product with many of the advantages contained in Epic's software, do so cheaply without years of time and monetary investment, and then sell that software to customers at a lower price than would otherwise be available if the software was developed without Epic's information.

(*Id.* at ¶ 12.)

Defendants do not directly dispute Martin's assessment of the documents, but offer their own expert's opinion that the majority of the sensitive documents are "User Guides or training materials and that all of the documents were of the type necessary for work of the TCoE testing team." (Defs.' Resp. to Pl.'s PFOFs (dkt. #308) ¶ 379 (citing Rept. of Erik Laykin (dkt. #189) pp.28, 77); *see also* Defs.' Add'l PFOFs (dkt. #300) ¶ 43.) Laykin goes even further, opining that "[n]one of the downloaded documents from UserWeb are overarching system and module descriptions that would enable a system designer to re-create the architecture [and] functionality." (Defs.' Add'l PFOFs (dkt. #300) ¶ 44 (citing Laykin Rept. (dkt. #189) p.77).)

iii. Evidence of TCS's use of Epic's documents

Putting aside the dispute between the parties' principal liability experts, a critical question as discussed below in the opinion, is whether TCS actually used the documents in their development of Med Mantra or other competitive products, or could still do so. TCS's corporate representative Syama Sundar testified at his deposition that there was no reason anyone on the Med Mantra team should "ever get any information that's confidential to Kaiser" or Epic. TCS further represents that all of the documents

---

training materials" (Defs.' PFOFs (dkt. #210) ¶ 132 (citing Laykin Rept. (dkt. #189) pp.28, 77)), but this does not directly dispute Epic's position that the files contain trade secrets.

downloaded from Epic's UserWeb were used solely for the purpose of performing services for Kaiser as part of the TCoE engagement. (*See also* Defs.' PFOFs (dkt. #210) ¶¶ 153-54 (Gajaram and Anandhan both testified at deposition that documents were only used for their Kaiser project work)).) TCS also maintains that it "found no copies of Epic documents on servers or computers used by TCS employees that work for Med Mantra or any other TCS software or work unrelated to Kaiser." (Defs.' Add'l PFOFs (dkt. #300) ¶ 48 (citing MacGregor Decl., Ex. 13 (dkt. #306-15) (TCS's Responses to Pl.'s First Set of Interrogatories)).)

In contrast, Epic disputes that TCS's limited search was sufficient to make this determination. (Pl.'s Resp. to Defs.' Add'l PFOFs (dkt. #381) ¶ 48.) Epic also offers some evidence of documents being used by TCS for purposes other than servicing the Kaiser account.[17] The court addresses this evidence by category.

a. Comparative Analysis

On March 5, 2014, Ramareddy Baddam, the Kaiser delivery manager for the Hyderabad operation of TCS, sent Naresh Yallapragada an email which provided in part:

> As discussed, Mukesh is the Delivery Manager for TCoE whose team has good knowledge on hospital operations product. Please connect with him on the initiative we discussed.

[17] Epic also points out that Gajaram sent documents downloaded from UserWeb to an individual outside of TCS, Ranjeet Kumar. (Pl.'s Resp. to Defs.' Add'l PFOFs (dkt. #381) ¶ 46.; *see also supra* Facts § C.i.) Even if this evidence does not support a finding that TCS used the documents improperly, it does rebut TCS's position that the documents were solely used for the purpose of performing services for Kaiser.

(Pl.'s PFOFs (dkt. #213) ¶ 397 (quoting Richmond Decl., Ex. 69 (dkt. #236-1)).) TCS acknowledges that Yallapragada was a functional consultant for the Med Mantra team until November 2013, at which point he left to work for a German client. Upon his return in March 2014, however, TCS maintains that Yallapragada was unassigned.[18] During that time, Yallapragada worked on the comparative analysis, which is described in more detail below.

Moreover, TCS points out that the "Mukesh" mentioned in the email is Mukesh Kumar, who, as discussed above, was the Kaiser delivery manager for TCS's TCoE. Kumar later testified at his deposition that the "hospital operations product" Baddam refers to in the email was the Kaiser account. Also, on March 5, 2014, Baddam emailed Kumar, that: "Dr. Naresh is a domain consultant and will be working on this initiative. . . . Please contact with the SMEs who can help him in this initiative." (Pl.'s PFOFs (dkt. #213) ¶ 399 (quoting Richmond Decl., Ex. 69 (dkt. #236-1)).) A "SME" or a "Subject Matter Expert" is a TCS employee who has developed knowledge of a particular

[18] Plaintiff contends that Muthuswami's declaration describing Yallapragada's changing role amounts to a "sham affidavit," because it conflicts with his earlier deposition testimony. (Pl.'s Reply to Pl.'s PFOFs (dkt. #382) ¶ 394 (quoting Muthuswami Depo. (dkt. #188) 188-189; Muthuswami Decl. (dkt. #271) ¶ 24).) Plaintiff is correct that "parties cannot thwart the purposes of Rule 56 by creating 'sham' issues of fact with affidavits that contradict their prior depositions." *Bank of Ill. v. Allied Signal Safety Restraint Sys.*, 75 F.3d 1162, 1168 (7th Cir. 1996). Here, however, Muthuswami's declaration does not contradict his earlier deposition testimony. In his deposition, Muthuswami testified that Yallapragada was on the Med Mantra team without any mention of the timeframe. In his declaration, Muthuswami simply clarifies that when Yallapragada was working on the comparative analysis, he was not, formally at least, assigned to the Med Mantra team. While there still may be a factual issue as to Yallapragada's role during the relevant time period between March and April 2014, the court will not strike Muthuswami's declaration. Instead, it will be up to the jury to determine Yallapragada's role during the relevant period.

application through his or her work on it. For example, the SMEs on the Kaiser TCoE team developed their knowledge of Kaiser and Epic software by working on it.

In a March 19, 2014, phone call, Yallapragada told Kumar that he would be sending him an excel spreadsheet for the SMEs on the Kaiser TCoE team to fill out and return to him. That same day, Kumar emailed Yallapragada three documents entitled, "Epic Architecture," "Epic and its Integration" and "KP HealthConnect Introduction and Overview." One of the documents contained flowcharts of the Kaiser HealthConnect software and discussed modules of the Epic software. (Pl.'s PFOFs (dkt. #213) ¶ 409 (citing Richmond Decl., Ex. 18 (dkt. #230)).) Another document was an introduction provided to new team members, which gave a basic overview of the HealthConnect software, including the "look and feel of the [Epic] software." (Pl.'s PFOFs (dkt. #213) ¶¶ 413-14 (citing Richmond Decl., Ex. 18 (dkt. #230)).) The documents also contained screenshots of Epic's software.

On March 21, Yallapragada emailed Baddam and attached a document entitled "Epic-Med Mantra comparative analysis." (Pl.'s PFOFs (dkt. #213) ¶ 416 (citing Richmond Decl., Ex. 74 (dkt. #236-6)).) In the email, Yallapragada said that this was a "first cut," which he will work to "take this analysis to the next level and come out with a concrete report." (*Id.*)

On March 24, Kumar sent an email to Vikran Vadamalai, a training manager for the Kaiser account, copying Yallapragada. Kumar asked Yallapragada to "have the SME[s] and Senior leads [c]onnect with Naresh today." (Pl.'s PFOFs (dkt. #213) ¶ 420

(quoting Richmond Decl., Ex. 75 (dkt. #236-7)).) Vadamalai responded that Yallapragada should call him that day and that he would have leads available.

Vadamalai then coordinated a group of SMEs to give an overview of HealthConnect, including Epic's modules, to Yallapragada. That same day, Vadamalai emailed Yallapragada and attached a document entitled "Epic Modules_Session Details." (Pl.'s PFOFs (dkt. #213) ¶ 424 (quoting Richmond Decl., Ex. 77 (dkt. #236-9)).) In that email, Vadamalai explained that the attachment contains a "list of sessions we have planned to conduct over the week to get yourself familiarized with the modules in EPIC." (Pl.'s PFOFs (dkt. 212) ¶ 425 (quoting Richmond Decl., Ex. 77 (dkt. #236-9)).)

Yallapragada also attended a "Web-ex" session with individuals who had one to one and a half years of experience with the Epic modules. For example, Srikanth Telkapalli was the SME for HealthConnect software for Kaiser's emergency department. Telkapalli testified at his deposition that he provided Yallapragada with the knowledge Telkapalli had gained through working on Epic.

On March 26, 2014, Yallapragada sent another email to Kumar attaching a document entitled "Epic product analysis." (Pl.'s PFOFs (dkt. #213) ¶ 431 (quoting Richmond Decl., Ex. 79 (dkt. #236-11)).) Yallapragada indicated that the attachment contained "a list of features of the modules covered so far," and he requested that Kumar assist in "filling up the sheet by specifying if the functionality is present in Epic or [n]ot." (Pl.'s PFOFs (dkt. #213) ¶¶ 432-33 (quoting Richmond Decl., Ex. 79 (dkt. #236-11)).) Yallapragada sent emails the following two days with updated lists. Kumar later testified at his deposition that if he had known Yallapragada was doing a comparative analysis, he

and his team "definitely . . . would have stopped" providing him information about Epic. (Pl.'s Add'l PFOFs (dkt. #415) ¶ 535 (quoting Kumar Depo. (dkt. #130) 98).)

On April 1, 2014, Yallapragada sent an email to Venugopal Reddy, Phillipe Guionnet and Baddam entitled "Epic-Med Mantra comparative analysis." (Pl.'s PFOFs (dkt. #213) ¶¶ 441-42 (quoting Richmond Decl., Exs. 83, 84 (dkt. ##236-15, 236-16)).)[19] The first page of the comparator analysis lists 33 different modules (*e.g.,* ADT, ambulance, billing, blood bank, human resources, nurses, etc.), and has two columns running parallel, labelled "EPIC" and "MED MANTRA." Each cell contains a "yes" or "no" reflecting whether the listed module is found in the particular software. Med Mantra has all 33 modules; Epic is missing 12 of the listed modules. Epic points out that the "EPIC" column also describes whether the particular module was being used by Kaiser. The next nine pages of the document contain a chart with five columns: module name; process name; sub process; availability in Epic; and remarks.[20]

TCS's Chief Security Officer Ajit Menon searched Yallapragada, Reddy, Kumar and Baddam's emails to determine whether they had emailed the document to others. His search revealed that Yallapragada had emailed the attachment to Baddam again on July 14, 2014, and Baddam then sent the email to Madhavi Mukherji, Madsusana Badarapu, and Bhavin Shah on July 21, 2014. Menon also looked to see if any of those

[19] TCS acknowledged that at some point Kumar also obtained a copy of this analysis.

[20] The parties dispute whether the information contained was "generic and could have been created based on general knowledge of healthcare software systems." (Pl.'s Resp. to Defs.' Add'l PFOFs (dkt. #381) ¶ 28; *see also* Pl.'s Add'l PFOFs (dkt. #415) ¶¶ 532-34 (citing deposition testimony of TCS employees stating that the comparative analysis was not based on generic information or that they have no basis for so stating.) The court takes up this dispute in its opinion below.

individuals had forwarded the comparative analysis, but found no indication that this was done. Epic does not dispute that Menon conducted these searches but disputes that his searches were adequate.

The parties also dispute whether Kumar, Reddy and Baddam were involved with Med Mantra. Epic points out that Reddy is listed on the organizational chart for Med Mantra as the "HC Delivery Head," and that he testified at his deposition that he provided "the administrative oversight to Med Mantra from a people perspective." (*Id.* at ¶ 29 (quoting Reddy Depo. (dkt. #159) 27; *see also* Pl.'s Add'l PFOFs (dkt. #415) ¶ 536.) In addition to be involved with Med Mantra, Guionnet testified that Reddy had a conflict of interest because "he was in charge of delivery [for Kaiser] and in that capacity he had access" to information about Epic software. (Pl.'s Add'l PFOFs (dkt. #415) ¶ 538 (quoting Guionnet Depo. (dkt. #156) 153).)[21]

Finally, the parties dispute *who* even requested the creation of the comparative analysis. Defendants maintain that Guionnet requested this particular analysis (purportedly based on his suspicion that TCS was using Epic's software to aid in its development of Med Mantra, *see infra* Facts § D.i). In late 2012 or early 2013, however, Reddy asked a TCS employee Vishwa ("DV") Prasad to "prepare a presentation comparing functionality between MedMantra Vs Epic Vs Cerner products and share it with him such that we can assess Me[d]Mantra and see if we directly sell Me[d]Mantra to Kaiser or make necessary changes and then go to Kaiser." (*Id.* at ¶ 31 (quoting Richmond Decl., Ex. 3 (dkt. #380-3)); *see also* Prasad Depo. (dkt. #349) 163-69.) When

[21] The court also will take up this dispute below.

Prasad told Reddy that he did not have access to Epic or Cerner software, Reddy asked Prasad to "sit with [his] team and . . . get their help in browsing through the functionality." (Pl.'s Add'l PFOFs (dkt. #415) (quoting Prasad Depo. (dkt. #349) 173).) Prasad also testified at his deposition that he informed his boss Venu Medikondra about the exchange with Reddy. [22] Prasad, however, declined to conduct the requested analysis.[23]

b. Beaker Documents

In addition to the comparative analysis, Epic also offers evidence that someone using Gajaram's credentials downloaded documents relating to Epic's laboratory program, "Beaker," on September 21, and 26, 2012. All of the downloads occurred in India. These documents could *not* have been used for TCS's work for Kaiser, since Kaiser does not use Epic's laboratory product. Epic also points out that around 2014, DaVita Kidney Care, a hospital in Colorado, began actively using a Med Mantra lab product developed for it by TCS. The development work for that software began in November 2011, shortly after Gajaram came to work for TCS with credentials to access Epic's UserWeb.

[22] Plaintiff points out that Reddy and Medikondra never mentioned Prasad or this requested analysis in their respective depositions. In fact, Reddy initially denied knowing Prasad. (Pl.'s Resp. to Defs.' Add'l PFOFs (dkt. #381) ¶ 31.)

[23] Prasad indicated that he declined to do this analysis because of discomfort with the ethics of using information about Epic's product gained solely for the purpose of servicing the Kaiser account.

D. Parties Learn of TCS's Access

i. Guionnet informs Kaiser, TCS and Epic about improper access

On April 20, 2014, Guionnet, as TCS's vendor engagement executive for Kaiser, wrote an email to Sundar as head of that account with the subject line "EPIC." (Defs.' Add'l PFOFs (dkt. #300) ¶ 11 (quoting MacGregor Decl., Ex. 9 (dkt. #306-11)).) The email goes on to detail Guionnet's concerns about TCS's improper access to Epic proprietary information.[24] On April 24, 2014, Guionnet also wrote to Suri Kant, President of TCS America, and Narasimhan Srinivasan, head of HR for North America, and requested information about contacting the TCS Audit Committee, whistleblower policies, and policies regarding harassment, discrimination, intimidation and coercion. Srinivasan responded and attempted to arrange a telephone meeting. On May 1, 2014, Guionnet wrote another email to Srinivasan that had a letter attached describing his "reasonably based suspicion" of some "illegal" activities and requesting additional information and an investigation. (*Id.* at ¶ 14 (quoting MacGregor Decl., Ex. 11 (dkt. #306-13)).)

On May 28, 2014, Guionnet sent an email to Kaiser employees stating that he believed he had a "duty to report 'reasonably based suspicion' of illegal activities affecting Kaiser." (Pl.'s PFOFs (dkt. #213) ¶ 446 (Richmond Decl., Ex. 85 (dkt. #236-17)).) On June 3, Guionnet sent a second email to individuals at Kaiser explaining that his

[24] Guionnet's concern appears to have been prompted by a February 2014 presentation he attended by the chief information officer for Apollo, during which he was surprised by significant developments with Med Mantra, raising a concern about unauthorized access and use of Epic's competing product information. Defendants point out that Guionnet had sent earlier emails to Muthuswami and Sundar without mentioning his suspicions, although a number of them pre-date this February 2014 presentation.

suspicion of illegal activity "related to the access to the EPIC software and/or to the Epic Portal by TCS at Kaiser and of Patent and/or Trademark Infringement, and/or Piracy, and/or misappropriation of Trade Secret, and/or tampering with [] Epic Intellectual property by TCS in order to benefit the TCS Software MedMantra." (*Id.* at ¶ 447 (Richmond Decl., Ex. 86 (dkt. #236-18)).) In that email, Guionnet further expressed his belief that TCS employees were using "fraudulent-obtained IDs" to access the Epic Portal in order to provide services to Kaiser. (*Id.* at ¶ 448 (Richmond Decl., Ex. 86 (dkt. #236-18)).) Moreover, Guionnet stated that: (1) TCS hired "2 years ago a CSC individual for the sole reason that he had a Kaiser ID that allowed him to access the Epic Portal"; and (2) TCS had "acquired fraudulently a second ID [a] few weeks ago in order to provide maintenance [and] support services from India." (*Id.* at ¶ 449 (Richmond Decl., Ex. 86 (dkt. #236-18)).) Finally, Guionnet stated that he believed Sundar had knowledge of this for months and possibly years.[25]

ii. TCS and Kaiser conduct investigations

On May 5, 2014, Srinivasan, in HR, responded to Guionnet by letter, stating that the nature of his concerns remained "unclear," but that a TCS investigator would be available to meet with Guionnet. On May 6, 2014, TCS also retained the law firm of Loeb & Loeb LLP to conduct an investigation into Guionnet's various allegations, a number of which involve issues not material to the present lawsuit. In May 2014, a

[25] On June 1, 2014, Guionnet sent an email containing similar allegations to certain TCS employees.

partner at Loeb & Loeb, Curt Bajak, requested to meet with Guionnet. Guionnet initially refused, but ultimately did meet with Bajak in late June 2014.

TCS management also requested that Ajit Menon, TCS Chief Security Officer, undertake the review of operations requested by Loeb & Loeb. Menon engaged Paul Amalraj, the Information Security Manager at TCS India and member of the Corporate Security Team, to carry out that review. As part of the investigation, TCS's internal team interviewed members of the on-shore and off-shore Kaiser team, and, on August 22, 2014, TCS employees Santosh Mohanty, Menon and Amalraj prepared an Assessment Report for Michelle La Mar, another partner with Loeb & Loeb.[26]

On June 12, 2014, David MacLeod, a member of the Kaiser compliance team, emailed Guionnet expressing his concerns about potential fraudulent activities. Guionnet responded on June 16, indicating that his concerns about "fraudulent access to EPIC" involve the servicing of the TCoE contract, as well as "benefiting Med Mantra." (Pl.'s PFOFs (dkt. #213) ¶ 456 (quoting Richmond Decl., Ex. 89 (dkt. #236-21)).)

On July 22, 2014, Kaiser also contacted Sundar to inform TCS formally of Guionnet's allegations. Following that conversation, Sundar then emailed TCS's CEO Chandra and Healthcare Group President Muthuswami to inform them of his conversation with Lisa Caplan, SVP of Care Delivery at Kaiser, who confirmed TCS that one of TCS's associates "had accessed EPIC materials which are not appropriate for the

[26] Plaintiff does not dispute that defendants undertook any of these actions, though it disputes that the actions, or the review more generally, was adequate. In particular, plaintiff points out that despite members of the security team testifying that any investigation should include reviewing employee access, computer and web proxy logs, defendants did not check these various logs in conducting its investigation. (Pl.'s Add'l PFOFs (dkt. #415) ¶¶ 692-95.)

role he is performing and he also shared his credentials (User ID and Password) with two others from TCS team." (Pl.'s PFOFs (dkt. #213) ¶ 458 (quoting Richmond Decl., Ex. 90 (dkt. #237)).) In that email, Sundar also reported that "[g]iven the severity of the security concern, [Kaiser] would like to conduct a very detailed review of the entire case and wanted to engage [TCS's] legal and HR teams to facilitate the complete investigation." (*Id.* at ¶ 459 (quoting Richmond Decl., Ex. 90 (dkt. #237)).) Finally, Sundar reported that Kaiser planned to transition Epic-related work from TCS.

On August 5, 2014, Kaiser's compliance team member MacLeod also sent a letter to Madhavi Mukherji as Guionnet's replacement on the Kaiser team after he was placed on leave, requesting TCS's assistance and cooperation with the investigation. On September 12, 2014, TCS's Information Security Manager Amalraj emailed MacLeod a document described as TCS's "assessment of the concerns raised by Kaiser." (*Id.* at ¶ 465 (quoting Richmond Decl., Ex. 41 (dkt. #232-9)).)[27] The report represented that "Epic User Web is not to be used by TCS associates, as TCS did not have a direct agreement with Epic." (*Id.* at ¶ 467 (quoting Richmond Decl., Ex. 41 (dkt. #232-9)).) Despite this understanding, the report acknowledged that: (1) the "TCS team did access the EPIC User Web portal"; and (2) "[c]ertain members within the TCS Kaiser team had shared credentials violating the laid down policies." (*Id.* at ¶ 469 (quoting Richmond Decl., Ex. 41 (dkt. #232-9)).)[28]

[27] Though not entirely clear, it appears this report is the same one involved in the Loeb & Loeb investigation headed by Menon.

[28] Plaintiff contends that this report also falsely claims that Pandurangan (referred to in the report as Ms. Deepa) created her own account, rather than acknowledging that her boss at TCS,

Gajaram admitted at his deposition that he originally lied to MacLeod about not sharing his credentials during Kaiser's initial investigation. While Gajaram eventually admitted that he had accessed the UserWeb, the TCS report indicates that he only did so "a few times." (*Id.* at ¶ 482 (quoting Richmond Decl., Ex. 41 (dkt. #232-9)).) Anandhan also admitted at his deposition that he lied to MacLeod about his team never using Gajaram's credentials and his never hearing of Pandurangan's access to the UserWeb.[29] Eventually Anandhan confessed to using Gajaram's credentials himself, but the TCS report still indicated that there was no evidence that he had "shared the credentials with anybody else within Kaiser or outside" (Pl.'s PFOFs (dkt. #213) ¶ 483 (quoting Richmond Decl., Ex. 41 (dkt. #232-9))), which later proved not to be true.

Even after TCS became aware that there *was* unauthorized access of the UserWeb, it did not inform Epic of this fact directly.[30] Around October 29, 2015, just shy of a year after Epic had filed this lawsuit, "TCS sent emails to all currently employed individuals [who] had been, during the relevant time, on the Northwest and National teams for the

---

Anandhan, created the account in her name without her knowledge. (*Id.* at ¶¶ 472, 474 (quoting Richmond Decl., Ex. 41 (dkt. #232-9)).)

[29] Defendants point out that Anandhan testified that he was "not completely truthful due to the fact that he was really [nervous] and had not met him before" (Defs.' Resp. to Pl.'s PFOFs (dkt. #308) ¶ 479), but this is of little or no moment for purposes of summary judgment.

[30] Defendants purport to dispute this proposed fact to the extent it implies that "the access in question was not permitted or that Epic was not already aware of the access." (Defs.' Resp. to Pl.'s PFOFs (dkt. #308) ¶ 488.) Defendants do not, however, put forth any evidence that it did, in fact, contact Epic. On the contrary, the account executive for Kaiser, Sundar, admitted at his deposition that TCS did not "reach out to Epic" after Kaiser informed TCS that there was unauthorized access. (Pl.'s PFOFs (dkt. #213) ¶ 489.) In his 30(b)(6) deposition, Muthuswami also testified that TCS did not alert Epic that passwords were shared, nor did TCS send the report that TCS prepared for Kaiser to Epic. Indeed, the report was not produced to Epic in discovery until September 16, 2015. Muthuswami also testified that he was not aware of any effort to this day to inform Epic in writing of TCS's access to the UserWeb.

TCoE engagement, and the IMG-Swat team for the Kaiser account." (Defs.' Add'l PFOFs (dkt. #381) ¶ 51.) In total TCS sent 80 emails and received 77 responses. (Defendants contend that the three individuals who did not respond are currently on leave.) The emails asked for the following information:

> (i) each employees' job title, role and Kaiser region services; (ii) whether the employee worked onshore or offshore; (iii) whether they obtained UserWeb credentials from anyone; (iv) if they responded yes . . ., who they received the credential from, whose credentials they were, whether they used it to access UserWeb, whether they used it to download documents from UserWeb, and if documents were downloaded, where they were saved; and (v) the employee's current location.

(Defs.' Add'l PFOFs (dkt. #300) ¶ 51.)

Plaintiff does not dispute that TCS took this (late) step, but disputes that it was a sufficient and adequate method to determine the extent of unauthorized use of its UserWeb. Through this investigation, TCS did learn that six individuals were issued UserWeb passwords either from Epic after completing an Epic training or from a Kaiser employee. (Defs.' Add'l PFOFs (dkt. #381) ¶¶ 52-57.) TCS also learned -- consistent with the description above (*see supra* Facts § C.i) -- that six other individuals used Gajaram's UserWeb credentials to access documents. Still, as plaintiff points out, a number of employees later testified at their deposition that they had lied about accessing the UserWeb in responding to the survey.[31] (Pl.'s Add'l PFOFs (dkt. #460) ¶¶ 674-79.)

[31] Plaintiff objects to defendants' use of these surveys as hearsay. (*See* Pl.'s Resp. to Defs.' Add'l PFOFs (dkt. #381) ¶ 52.) The court does not, however, consider the survey for the truth of the matter asserted, especially since some of the employees who responded later recanted under earth. Rather, it is considered as proof that TCS conducted a survey.

iii. Epic's investigation

On June 3, 2014, Guionnet informed Epic of his "'reasonably based suspicion' of 'illegal activity' and fraud related to the access to the EPIC Software and/or to the EPIC Portal by TCS at Kaiser and of Patent and/or Trademark infringement, and/or Piracy, and/or misappropriation of Trade Secret, and/or tampering with [] EPIC intellectual property by TCS in order to benefit the TCS Software MedMantra." (Pl.'s PFOFs (dkt. #213) (quoting Richmond Decl., Ex. 96 (dkt. #237-6)).)

As part of Epic's follow-up investigation, its expert "spent a tremendous amount of [personnel] energy investing in understanding what had happened, investing in understanding what had happened, building the tools and utilities . . . to connect and correlate the web access logs with the download history . . . [to] understand where accesses were occurring from." (*Id.* at ¶ 504 (quoting Stirling Depo. (dkt. #186) 163).) While defendants dispute that this effort took a "tremendous amount of personnel energy" (Defs.' Resp. to Pl.'s PFOFs (dkt. #308) ¶ 504), they provide no counter evidence in the form of expert testimony or otherwise to challenge Epic's description. Plaintiff also details its efforts, including: understanding who else had registered for the UserWeb; building new tools to correlate the web access with where people were located geographically; and developing the details about the downloaded documents. Plaintiff's expert estimates that Epic personnel spent approximately 108 hours investigating TCS's unauthorized downloading of Epic information, which amounts to losses exceeding $9,000. Defendants dispute this assessment based on the lack of documentation of the

hours spent and Epic's failure to substantiate that figure. (Defs.' Add'l PFOFs (dkt. #381) ¶ 68.)[32]

Consistent with the above description, Epic's investigation did reveal that through the use of Gajaram's account, thousands of documents and over 1,680 unique files were downloaded. Epic's investigation further revealed that the credentials were used to access the UserWeb outside of Oregon -- where Gajaram was located for at least some of the relevant time period -- including from locations in India.

OPINION

Both parties filed motions for summary judgment. Summary judgment is appropriate if the moving party "shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). "The party pursuing the motion must make an initial showing that the agreed-upon facts support a judgment in its favor." *Hotel 71 Mezz Lender LLC v. Nat'l Retirement Fund*, 778 F.3d 593, 601 (7th Cir. 2015) (citing Fed. R. Civ. P. 56(a), (c)(1); *Celotex Corp. v. Catrett*, 477 U.S. 317, 323-24 (1986)).

Plaintiff seeks a finding of liability on four claims: (1) breach of contract; (2) breach of duty of good faith and fair dealing (as an alternative to its breach of contact claim); (3) violation of the Computer Fraud and Abuse Act, 19 U.S.C. §1030(g); and (4)

[32] Defendants also argue that there is no evidence that TCS employees "modified or otherwise impaired any documents on the UserWeb," "impaired data on UserWeb," "affected the availability of UserWeb," or "interrupted UserWeb service." (Defs.' PFOFs (dkt. #210) ¶¶ 133-39.) As the court explained in its decision on defendants' motion to dismiss and will explain further below, however, such a finding is not required to demonstrate loss under the CFAA. (*See* 11/18/15 Op. & Order (dkt. #243) 9-13; *infra* Opinion § I.B.)

violation of the Wisconsin Computer Crimes Act, Wis. Stat. § 943.70(2)(a). Defendants seek judgment on those same claims, as well as other claims asserted in plaintiff's complaint. The court will begin with the merits of plaintiff's motion, and then will turn to the remaining state law claims for which defendants seek judgment in their favor.

I. Plaintiff's Motion for Summary Judgment

Since plaintiff seeks summary judgment on claims for which *it* bears the burden of proof, "it must lay out the elements of the claim, cite the facts which it believes satisfies these elements, and demonstrate why the record is so one-sided as to rule out the prospect of a finding in favor of the non-movant on the claim." *Hotel 71 Mezz Lender LLC*, 778 F.3d at 601; *see also Reserve Supply Corp. v. Owens-Corning Fiberglas Corp.*, 971 F.2d 37, 42 (7th Cir. 1992) ("[B]ecause Owens-Corning and CertainTeed also have the burden at trial of establishing good faith, they must establish affirmatively the lack of 'sufficient evidence favoring the nonmoving party for a jury to return a verdict for that party.'" (quoting *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 249-50 (1986))). "If the movant has failed to make this initial showing, the court is obligated to deny the motion." *Hotel 71 Mezz Lender LLC*, 778 F.3d at 601; *see also Johnson v. Hix Wrecker Serv., Inc.*, 651 F.3d 658, 662 (7th Cir. 2011) ("A party opposing summary judgment does not have to rebut factual propositions on which the movant bears the burden of proof and that the movant has not properly supported in the first instance.").

A. Breach of Contract Claim and Breach of Duty of Good Faith and Fair Dealing Claim

Although both sound in contract under Wisconsin law, plaintiff alleges claims for breach of its 2005 Agreement with defendants and, if the court were to find that plaintiff had failed to prove a breach of a specific term of the 2005 Agreement, for breach of duty of good faith and fair dealing. The court will, therefore, address plaintiff's claim that defendants breached specific contract provisions first.

"The elements for a breach of contract in Wisconsin are familiar; the plaintiff must show [1] a valid contract that [2] the defendant breached and [3] damages flowing from that breach." *Matthews v. Wis. Energy Corp.*, 534 F.3d 547, 553 (7th Cir. 2008) (citing *Nw. Motor Car, Inc. v. Pope*, 51 Wis. 2d 292, 296, 187 N.W.2d 200 (1971)). With respect to the first element, there is no dispute that the 2005 Agreement is enforceable, unambiguous, and was not modified. (*See supra* Facts § B.ii.)[33]

As for proof of the second element, plaintiff posits three ways in which TCS breached the contract. *First*, plaintiff contends that TCS breached the Agreement by (a) failing to "[l]imit access to the Program Property to those of [its] employees who must have access to the Program Property in order to implement the Program Property on Epic's or its customer's behalf," and, relatedly, (b) failing to "[u]se any Confidential Information only for the purpose of implementing the Program Property on an Epic customer's behalf." (Richmond Decl., Ex. 20 (dkt. #230-2) 3.) In support of this claim (*i.e.*, using the documents for a purpose other than TCS's work for Kaiser), plaintiff

[33] By not addressing this first element, defendant essentially concede the existence of a valid contract. *See Wojtas v. Capital Guardian Trust Co.*, 477 F.3d 924, 926 (7th Cir. 2007) (failure to oppose arguments raised on motion for summary judgment constitutes waiver).

principally argues that since defendants admit access to the UserWeb was not necessary to perform its work, accessing and downloading of UserWeb documents demonstrates improper use. (*See supra* Facts § B.v.) That TCS need not have had access to the UserWeb to perform its work for Kaiser, however, does not demonstrate that the documents TCS employees accessed and downloaded from the UserWeb were used for an impermissible purpose (*i.e.*, a purpose other than to further TCS's work for Kaiser). While a reasonable fact finder might well infer an impermissible purpose based on all of the circumstantial evidence here, an admission that access was unnecessary does not foreclose a jury finding that TCS's access (and even downloads from) the UserWeb was for the purpose of performing work for its customer Kaiser.

Plaintiff also points to TCS's development of a comparative analysis as evidence of misuse. Here, however, plaintiff lacks direct evidence that the analysis was developed using Epic documents from the UserWeb. While there is no dispute that members of the Kaiser team, in particular Mukesh Kumar and his team members, were involved in providing information to Yallapragada and others about Epic modules (*see supra* Facts § C.iii.a), plaintiff would need the jury to infer that the comparative analysis report was prepared from confidential Epic documents, rather than from the knowledge of Kaiser team members *or* from other individuals' general, public knowledge about Epic and its products.

This is not to say that plaintiff has failed to come forward with sufficient circumstantial evidence for a reasonable jury to make this inference, only that a factual dispute exists as to the source of the comparison. Of course, the evidence is further

muddled by uncertainty over the reason behind the comparison, since TCS whistleblower Guionnet *may* have requested (or at least caused) the comparative analysis in an effort to confirm (or disprove) his own suspicion that Med Mantra benefited from knowledge of Epic's products through TCS's work with Kaiser.[34]

In its reply, plaintiff spends several pages describing TCS employee DV Prasad's involvement in an earlier effort to create a comparative analysis. In that instance, yet another TCS employee, Venugopal Reddy, was interested in using the Kaiser team and their access to Epic materials to create a comparative analysis for the express purpose of developing a competing product to sell to Kaiser. (*See supra* Facts § C.iii.a.) Certainly, Prasad's testimony and supporting evidence appears to be circumstantial proof of TCS's interest in accessing UserWeb documents for the improper purpose of furthering TCS's own software development (at least in late 2012 or early 2013), but there is neither definitive evidence that TCS did so for this purpose, nor that it used Epic documents to develop that analysis. Whether this evidence of TCS's interest in creating a comparative analysis for competitive purposes, along with evidence of its actual, unauthorized access to confidential information that would be useful for that purpose, is enough to infer improper use with respect to the 2014 competitive analysis remains a question for the jury.

Finally, plaintiff points to evidence of TCS's downloading of the "Beaker" documents, which describe Epic's laboratory module, as proof of improper use. Tellingly,

[34] Perhaps Guionnet's investigation would be an improper use, though this is unclear on the present record. In any event, it is not the improper use Epic is asking the court to infer: development of a competitive software program.

defendants offer *no* explanation or other response to this evidence. Instead, defendants simply stand by the general statement that documents accessed from the UserWeb simply furthered TCS's work for Kaiser. Even coupled with the fact that TCS developed a lab software product for a hospital in Colorado around the same time, however, proof of access to the Beaker documents does not constitute *definitive* evidence of TCS's improper use. Again, the jury will need to weigh the significance of this evidence and draw adverse inferences to find in plaintiff's favor. Accordingly, the court will deny plaintiff's motion for summary judgment on its breach of two, specific contract terms that turn on disputed evidence of improper use.

Second, plaintiff argues that TCS breached the Agreement by failing to "[n]otify Epic promptly and fully in writing of any person, corporation or other entity that [it] know[s] has copied or obtained possession of or access to any of the Program Property without authorization from Epic." (Richmond Decl., Ex. 20 (dkt. #230-2) 3.) Unlike the first two theories, here, plaintiff has produced undisputed evidence of a breach. Specifically, there is no dispute that TCS, even to this day, has failed to provide written notice to Epic as required under the Agreement of its employees unauthorized and improper access to the UserWeb.

In response, defendants simply argue that that they had no contractual obligation to notify Epic since the information accessed was not used improperly. But this argument misses the mark. Leaving aside the material disputed facts about improper use, the plain language of the 2005 Agreement does not require improper *use* to trigger TCS's obligations. Instead, all that is required is improper *access* to documents and a failure to

notify. Here, there is no dispute that a number of TCS employees gained unauthorized access to Epic's UserWeb and improperly copies documents repeatedly over a two year period. Not only did TCS not give *prompt* notice of its surreptitious and unauthorized access and possession of Epic proprietary information, it gave *no* notice.

Ironically, defendants contend that whistleblower Guionnet's June 2014 email to Epic satisfied the notice requirement, but that notice was neither prompt nor full as required by the parties' Agreement. Defendants' argument that Epic had *constructive* notice of Gajaram's use given his disclosure in December 2012 that he had become a TCS employee has only slightly more merit, since it ignores damning, undisputed facts on this record, including that: (1) Gajaram's own use from September 2011 to December 2012 without notifying Epic of his change in employment *or* the location of his employment; (2) other individuals use Gajaram's credentials to access UserWeb documents; and (3) the work around to renew Gajaram's credentials and at least one other individual's credentials to continue improper access. Since TCS neither promptly nor fully disclosed these facts either, TCS repeatedly breached the terms of its 2005 Agreement with Epic.

Third, and finally, plaintiff contends that TCS breached the 2005 Agreement by failing to "maintain in confidence any Confidential Information" and failing to "[s]tore all copies of the Program Property in secure place." (Richmond Decl., Ex. 20 (dkt. #230-2) 2-3.) In support of this theory, plaintiff points to TCS's undisputed failure to comply with Kaiser's security proposals by having its own kiosk computers in Kaiser's otherwise secure ODCs, which gave TCS access to the internet and TCS email. Moreover, TCS

employees *admitted* transmitting Epic documents from the UserWeb using these computers to TCS email accounts, as well as saving documents to a so-called TCS "knowledge repository" for further use. (*See supra* Facts § C.i.) This evidence is arguably compelling enough to enter summary judgment in plaintiff's favor, but defendants can at least argue that it took steps to "maintain in confidence" and store copies "in a secure place." The court will, therefore, allow a jury to assess the evidence and determine whether TCS's lapses in security measures violate these provisions of the Agreement.[35]

At the same time, the court agrees that Gajaram's emailing of UserWeb documents outside of TCS constitutes a plain breach of the Agreement. Indeed, defendants' only response is that the recipient of the documents, Ranjeet Kumar, was "testing or implementing Epic software on behalf of Kaiser." (Defs.' Opp'n (dkt. #298) 23 n.6.) While perhaps true, it is at least a technical breach of the contract, since the Agreement only provides an exception for TCS's release of confidential information to Epic's licensee (here, Kaiser), not to another consultant like Kumar.

While there are factual disputes with respect to some of plaintiff's breach of contract theories, there is, therefore, no dispute that defendants breached the Agreement by failing to: (1) provide written notice of repeated unauthorized access as required under the contract; and (2) based on the undisputed fact that Gajaram emailed a document downloaded from the UserWeb to an individual outside of TCS, maintain in confidence information and store copies in a secure place. The court's finding of a breach

[35] Unlike TCS's gross lapses in prompt and full disclosure of its ongoing, unauthorized access to secured documents on Epic's UserWeb, it also remains to be proven that these lapses in security constitute *material* breaches.

as to those two specific theories does not foreclose Epic from pressing its other theories of breach at trial -- especially if those breaches would be material and result in damages.

This brings the court to the third element of plaintiff's claim: "damages flowing from that breach." *Matthews*, 534 F.3d at 553. Plaintiff contends that the court can enter partial judgment on the first two elements and "leav[e] damages to be established at trial." (Pl.'s Opening Br. (dkt. #212) 20.) Plaintiff also contends that it is entitled to judgment on its breach of contract claim, even if it cannot establish actual damages. (*Id.* at 20 n.4 (citing *Hydrite Chem. Co. v. Calumet Lubricants Co.*, 47 F.3d 887, 891 (7th Cir. 1995) ("Proof of liability is complete when the breach of contract is shown [and] [a]t that point the plaintiff is entitled to nominal damages."); *Olympia Hotels Corp. v. Johnson Wax Dev. Corp.*, 908 F.2d 1363, 1372 (7th Cir. 1990) ("The victim of a breach of contract is always entitled to nominal damages if he proves a breach but no damages.")).)[36]

Defendants largely ignores this argument, simply citing to an unpublished case from the Eastern District, which explains that "[w]here the issue has been presented on a

[36] Initially, the court questioned whether these Seventh Circuit cases -- *Hydrite Chemical Company* and *Olympia Hotels Corporation* -- held that a plaintiff in a breach of contract claim need not prove damages, as distinct from injury, to establish liability for breach of contract and award nominal damages. A careful reading of those cases -- in particular, the court's contrasting of a contract claim with a tort claim, where injury is required to find liability-- makes clear that a showing of injury is not required if a plaintiff simply seeks an award of nominal damages. *See Hydrite Chem. Co.*, 47 F.3d at 890-91 ("Liability in a contract case . . . does not depend on proof of injury."); *Olympia Hotels Corp.*, 908 F.3d at 1372 (contrasting breach of contract claim with that of a tort claim, and explaining that harm is required to demonstrate a tort). Another way to think of the distinction between a breach of contract that results in an injury and one that does not is to consider the distinction between a material and technical breach. *See generally* II Michael B. Apfeld *et al.*, *Contract Law in Wisconsin*, Ch. 12 p.31 (4th ed. 2013) ("A technical breach exists when a party has not absolutely complied with the contract, but the breach is found to have been harmless and would not constitute grounds for a claim for damages.") (citing cases finding award of nominal damages appropriate).

motion for summary judgment[,] plaintiff must prove damages to go to trial on a breach of contract claim." (Defs.' Opp'n (dkt. #298) 16 n.3 (citing *Centr. Brown Cnty. Water Auth. v. Consoer, Townsend, Envirodyne*, No. 09-C-0131, 2013 WL 501419, at *7 (E.D. Wis. Feb. 11, 2013)).) The court reads the *Central Brown County Water Authority* opinion as standing for the obvious proposition that there is no reason for a trial if plaintiff cannot prove any damages. Regardless of whether this is a correct reading, the case is distinguishable here because there is *no* dispute on the above-identified theories that defendants breached the contract. As such, there is no need for a trial on whether TCS breached these provisions, unlike the claims at issue in *Central Brown County Water Authority*.

Instead, the only issues for trial here on the above-identified theories, if plaintiff opts to proceed, are whether plaintiff was injured by the breach and its damages based on that injury. Of course, plaintiff may also proceed to trial on those theories for which the court has not entered judgment in its favor, including plaintiff's claims that defendants breached the 2005 Agreement by failing to (1) limit access or solely use UserWeb documents for Kaiser's behalf or (2) maintain in confidence and store copies in a safe place based on the inadequacy of TCS's security measures. At trial, plaintiff may pursue these claims by demonstrating a breach of those provisions and resulting damages.

As for plaintiff's alternative claim for breach of duty of good faith and fair dealing, the court's previous rulings dictates the outcome, either because its finding of a breach on the summary judgment renders the claim duplicative or the same disputed fact issues that precluded entry of judgment in plaintiff's favor also preclude a finding for breach of the

duty of good faith and fair dealing. Specifically, in order to demonstrate that defendants violated the "spirit" of the other provisions of the contract, *Springbrook Software, Inc. v. Douglas Cnty.*, No. 13-CV-760-SLC, 2015 WL 2248449, at *18 (W.D. Wis. May 13, 2015), plaintiff would have to demonstrate some sort of improper use or the inadequacy of TCS's security measures.

If plaintiff were to prove these facts at trial, it seems unlikely that a jury would not find a breach of the relevant contract provisions, which would again render these alternative claims duplicative, but the court will allow plaintiff to continue to pursue its alternative breach of duty of good faith and fair dealing claim at trial as well.[37]

B. CFAA Claim

Next, plaintiff seeks summary judgment on its Computer Fraud and Abuse Act claim. To prevail on a civil claim under the CFAA, Epic must prove that TCS (i) violated the CFAA, and (ii) caused Epic "damage or loss" amounting to at least $5,000. 18 U.S.C. § 1030(g) (providing private right of action by "[a]ny person who suffers damage or loss by reason of a violation of this section"); 18 U.S.C. § 1030(c)(4)(A)(i)(I) (requiring $5,000 loss).

Plaintiff maintains that defendants violated the CFAA by "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from a protected computer." 18 U.S.C. § 1030(a)(2). The term "protected computer" is defined as "a computer . . . which is used

[37] At this stage, plaintiff does not appear to have a theory to support its breach of duty of good faith and fair dealing claim that does not implicate TCS's specific obligations under the Agreement, but this is not before the court now and can in any event be sorted out before or at trial.

in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2).

Plaintiff points out that it is undisputed TCS employees accessed the UserWeb without authorization. Defendants dance around this point by arguing that the 2005 Agreement allowed Epic to use confidential information for Kaiser's purpose and that Kaiser (and even an Epic employee) sent TCS documents from the UserWeb. While this may well be relevant as to whether Epic incurred any damages due to TCS's violation of the CFAA, it is not material to the question of liability under that Act. For the reasons already explained above, there is no dispute that TCS at least "exceeded its authorization" when its employees intentionally and directly obtained information (namely, Epic documents) from the UserWeb. Nor does TCS dispute that the UserWeb (or the server which houses it) falls within the broad definition of "protected computer" under the CFAA. *See* 18 U.S.C. § 1030(a)(2) (requiring that to qualify as a "protected computer" it must be "used in or affecting interstate or foreign commerce . . . of the United States"); *see also LCRV Holdings, LLC v. Brekka*, 581 F.3d 1127, 1136 (9th Cir. 2009) (reviewing CFAA claim based on allegations that defendant "accessed [plaintiff's] information on a LOAD website after he left the company"); *Patrick Patterson Custom Homes, Inc. v. Bach*, 586 F. Supp. 2d 1026, 1032-33 (N.D. Ill. 2008) ("[A] computer that

provides access to worldwide communications through applications through the internet qualifies as a protected computer.").[38]

Plaintiff also contends that it has established more than $5,000 in losses caused by this violation as a matter of undisputed fact. In its original brief in support of its motion for summary judgment, defendants reiterate arguments raised in their motion to dismiss. The court will not repeat its holding, other than to note that Epic need only demonstrate damages *or* loss (not both), and that, for purposes of demonstrating a $5,000 loss under the CFAA, the cost of an investigation counts, even if that investigation does not involve the impairment or interruption of services. (11/18/15 Op. & Order (dkt. #243) 10, 12-13.)[39]

Here, plaintiff submits evidence from a senior vice president and the interim chief security officer, Stirling Martin, who claims more than $9,000 in costs in investigating the improper access. Defendants challenge Martin's estimate based on lack of documentation of the hours spent, as well as Martin's purported failure to substantiate the figure during his 30(b)(6) deposition. The court finds this evidence is not so one-sided as to warrant entry of judgment in plaintiff's favor. TCS has a right to question Martin about how he came up with the $9,000 amount, and then for a jury determination as to whether Epic's analysis is sufficient to find a loss of more than

[38] TCS has raised a genuine issue of material fact as to Gajaram's authority to access the UserWeb, at least after he informed Epic that he was a TCS employee in December 2012, but there is no dispute that other TCS employees lacked *any* authority to use Gajaram's credentials to access the UserWeb.

[39] In defendants' reply in support of its own motion for summary judgment (filed after the court issued its opinion on the motion to dismiss), TCS concedes this much at least for summary judgment, although TCS remains free to challenge this interpretation of the statute in any appeal.

$5,000. Moreover, this same testimony will be relevant in assessing damages for defendants' violation of § 1030(g).

Accordingly, the court will enter summary judgment in plaintiff's favor on an *element* of the CFAA claim, but will require plaintiff to prove at least a $5,000 loss during the damages phase of trial.

C. Wisconsin Computer Crimes Act Claim

In addition to the federal claim, plaintiff also asserts a claim under the Wisconsin Computer Crimes Act, Wis. Stat. § 943.70(2)(a) ("WCCA"). That act makes it unlawful to "willfully, knowingly and without authorization" (1) access, take possession of, or copy "computer programs or supporting documentation"; or (2) disclose "restricted access codes or other restricted access information to unauthorized persons."

For the same reasons the court found a violation of the CFAA based on undisputed evidence of defendants having accessed Epic's UserWeb without authorization (or in a manner which exceeds authorized access), the court finds that there is no dispute that a number of TCS employees willfully, knowingly and without authorization accessed, downloaded and copied documents from the UserWeb in violation of the WCCA. Even if there were disputed facts as to this prong, there is no dispute that TCS employee Gajaram disclosed his UserWeb credentials to other TCS employees, none of whom were authorized to access the UserWeb. Given that the WCCA also prohibits disclosing restricted codes and that plaintiff need not demonstrate loss or damage, entry of summary judgment in plaintiff's favor on this claim is an even easier call than entry on the first element of the CFAA claim.

Defendants also argue that plaintiff's Computer Crimes Act claim is preempted by Wisconsin's Uniform Trade Secrets Act ("UTSA"). (Defs.' Opp'n (dkt. #298) 27 (quoting Wis. Stat. § 134.90(6)(a) (The UTSA "displaces conflicting tort law, restitutionary law and other law of [Wisconsin] providing a civil remedy for misappropriation of a trade secret.")).) If all of the documents were claimed trade secrets, defendants' preemption argument would have merit, but defendants completely ignore the fact that while some of Epic's documents are trade secrets, the vast majority are not. As such, Epic's WCCA claim based on the downloading of approximately 1,572 documents for which Epic does *not* claim trade secret protection may proceed. *See Burbank Grease Servs., LLC v. Sokolowski*, 2006 WI 103, ¶ 33, 294 Wis. 2d 274, 717 N.W.2d 781 ("[A]ny civil tort claim not grounded in a trade secret, as defined in the statute, remains available." (emphasis removed)).[40]

On the other hand, as far as the court can discern, the only available remedy for a violation of the WCCA is injunctive relief, *see* Wis. Stat. § 943.70(5), and plaintiff has failed to direct the court to any need for prospective relief. In light of the undisputed record, the court will, therefore, enter judgment in plaintiff's favor on its Wisconsin Computer Crimes Act claim, while leaving open the question of what relief, if any, is appropriate for this violation.

[40] For the same reason, the court rejects defendants' similar argument raised in their own motion with respect to other state law claims. (*See* Defs.' Opening Br. (dkt. #214) 39-42 (listing claims).) Unless based on the trade secret documents, plaintiff's claims under Wisconsin law are not preempted by the UTSA.

II. TCS's Motion for Summary Judgment

The standard of review in assessing defendants' motion differs from that applied above in considering plaintiff's motion. The party moving for summary judgment bears the initial burden of showing there is no genuine issue of material fact and that it is entitled to relief. *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). Once this initial burden is met on an issue for which a nonmoving party will bear the burden of proof at trial, however, that party must "go beyond the pleadings" and "designate 'specific facts showing that there is a genuine issue for trial.'" *Id.* at 324.

The nonmoving party may not "simply show some metaphysical doubt as to the material facts." *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586 (1986). Rather, the nonmoving party must produce "evidence . . . such that a reasonable jury could return a verdict for the nonmoving party." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). If it fails to do so, "[t]he moving party is 'entitled to a judgment as a matter of law.'" *Celotex*, 477 U.S. at 323 (quoting Fed. R. Civ. P. 56(c)).

Defendants seek partial judgment on the same claims for which plaintiff has moved, as well as an array of additional claims. The court will not reiterate the parties' arguments or the court's analysis presented above, other than to note that on those claims for which the court has granted plaintiff's motion for summary judgment, the court necessarily will deny defendants' motion. For reasons explained below, the court's previous finding of disputed facts that foreclose a finding in plaintiff's favor on certain claims also precludes entry of judgment in defendants' favor.

A. Fraud Claim

To prove a claim of fraud under Wisconsin law, plaintiff must demonstrate the following five elements: (1) that defendant made a material representation, (2) that it was false; (3) that the plaintiff "believed and relied on the misrepresentation to his detriment or damage"; (4) that the defendant made the misrepresentation "with knowledge that it was false or recklessly without caring whether it was true or false"; and (5) that the defendant "made the misrepresentation with intent to deceive and to induce the plaintiff to act on it to his detriment or damage." *Tietsworth v. Harley-Davidson, Inc.*, 2004 WI 32, ¶ 13, 270 Wis. 2d 146, 677 N.W.2d 233.[41] Here, defendants offer two, independent bases for granting summary judgment in their favor on plaintiff's fraud claim. First, defendants argue that plaintiff cannot demonstrate that Gajaram made a false representation. Second, defendants contend that even if there were a misrepresentation, Epic cannot demonstrate that its reliance was reasonable. The court addresses each argument in turn.

i. False Representation

In its opening brief, defendants focus on the lack of any evidence that Gajaram made a false representation in his application for UserWeb access. (Defs.' Opening Br. (dkt. #214) 30-32.) Specifically, defendants contend it is undisputed that: (1) Gajaram was granted access as a CSC employee; (2) Gajaram informed Epic that he was a TCS

[41] Defendants point out that the standard of proof for a fraud claim under Wisconsin law is clear and convincing proof. (Defs.' Opening Br. (dkt. #214) 29 (citing *SJ Props. Suites v. STJ, P.C.*, 759 F. Supp. 2d 1032, 1043 (E.D. Wis. 2015)).) While correct and certainly material, the standard does not alter the outcome at summary judgment since the evidence plaintiff puts forth of both a misrepresentation and its reasonable reliance on that misrepresentation could satisfy the heightened standard of clear and convincing evidence.

employee in December 2012; and (3) he continued to do so in every resubmission after that until his account was terminated in June 2014.

As plaintiff points out in its opposition, defendants' framing of defendants' fraudulent conduct is misleadingly narrow. At the outset, defendants fail to note that Gajaram was employed by TCS and used and shared his UserWeb credentials for about 15 months (from September 2011 until December 2012), before informing Epic of his change in employment and then did so in a way that failed to flag the import in his change of status.[42] Leaving this context aside, defendants' motion completely ignores numerous misrepresentations by other TCS employees in using Gajaram's UserWeb credentials and in applying for an account for Pandurangan without her knowledge or consent.

Given that defendants ignored this entire category of misrepresentations, plaintiff argues that defendants' motion for summary judgment must be denied. Specifically, plaintiff points out that other employees including Anandhan and Gunasekaran, affirmatively misrepresented their identities to Epic in using Gajaram's credentials: "When anyone accessing UserWeb with Mr. Gajaram's credentials was not actually Ramesh Gajaram, such representations were indisputably false." (Pl.'s Opp'n (dkt. #414) 46.) Moreover, plaintiff points out that "TCS employees made false representations by registering for an account in Deepa Pandurangan's name without her

[42] While it appears that Gajaram was not *asked* by Epic for this information until December 2012, the court leaves for trial what duty, if any, defendants may have had to disclose Gajaram's hiring, including any earlier obligation to verify his status, whether because of its knowledge of Epic's ongoing concern or of Gajaram's explicit or implicit misrepresentations in originally obtaining his credentials as a Kaiser employee, reinstating his credentials after Epic learned of his employment by TCS or failing to update his employment status until asked to do so by Epic.

knowledge." (*Id.*) In doing so, those employees misrepresented their identity, as well as misrepresented that Pandurangan had read and agreed to abide by Epic's UserWeb Access Agreement.

In its reply, defendants effectively punt on these additional misrepresentations and reiterate instead its original framing of plaintiff's claim, pointing out that Epic was aware of Gajaram's employment with TCS. Putting aside the undisputed fact that Epic was not aware of this fact from September 2011 to December 2012, defendants still offer no response to evidence that other employees used Gajaram's and Pandurangan's credentials under false pretenses. Accordingly, the court finds that plaintiff has offered sufficient evidence of a genuine issue of material fact to overcome defendants' summary judgment motion as to whether their employees made false representations to access Epic's UserWeb.

ii. Reasonable Reliance

Defendants also seek summary judgment on the basis that plaintiff could not have reasonably relied on any alleged misrepresentations. "The general rule in Wisconsin, as elsewhere, is that the recipient of a fraudulent misrepresentation is justified in relying on it, unless the falsity is actually known or is obvious to ordinary observation." *Hennig v. Ahearn*, 230 Wis. 2d 149, 170, 601 N.W.2d 14, 24 (Ct. App. 1999). Here, defendants contend that any misrepresentation was obvious because Epic knew Gajaram worked for TCS. As discussed above, this is a non-starter since plaintiff opposes defendants' motion based on evidence that *other* employees made misrepresentations by using either Gajaram's or Pandurangan's account and by fraudulently setting up Pandurangan's

account in the first place. Defendants also fail to offer any response to this argument in its reply.

Because plaintiff's claim is premised on the alleged misrepresentations of other TCS employees, it need not demonstrate that any reliance on Gajaram's past employer was reasonable. Instead, the question at trial will turn on whether plaintiff's reliance on individuals to identify themselves truthfully was reasonable.[43] The court, therefore, will deny defendants' motion for summary judgment, finding that plaintiff offered sufficient evidence to raise a genuine issue of material fact as to both alleged false representations and its reasonable reliance on those representations.

B. Wisconsin Uniform Trade Secrets Act Claim

Defendants further move for summary judgment on plaintiff's claim under Wisconsin Uniform Trade Secrets Act, Wis. Stat. § 134.90(2), contending that plaintiff failed to put forth evidence of any actionable misappropriation. Plaintiff's claim is based on 36 of the 1,600 documents downloaded from the UserWeb, each of which it claims as trade secrets. At least at summary judgment, defendants do not dispute the characterization of these documents. Instead, defendants contend that there is no evidence of their being "misappropriated."

Plaintiff can demonstrate misappropriation in one of two ways. *First*, under subsection (a), misappropriation occurs when one "acquir[es] the trade secret of another

[43] In its opposition, of course, plaintiff also contends that it *was* reasonable to rely on those logging into the UserWeb to identify themselves correctly. At minimum, plaintiff raises a genuine issue of material fact as to whether its reliance was reasonable. TCS, of course, may introduce evidence of the laxness of security protocols to challenge Epic's position.

by means which the person knows or has reason to know constitute improper means." Wis. Stat. § 134.90(2)(a). "'Improper means' includes espionage, theft, bribery, misrepresentation and breach or inducement of a breach of duty to maintain secrecy." Wis. Stat. § 134.90(1)(a). Here, defendants largely regurgitate their argument in support of summary judgment on plaintiff's fraud claim, arguing that the undisputed record demonstrates Gajaram did not misrepresent his identity as a TCS employee when he logged into the UserWeb. Since there is evidence of other TCS employees misrepresenting themselves as Gajaram in order to access and download UserWeb documents, including the 36 documents containing trade secrets, the court finds that plaintiff has raised a genuine issue of material fact as to whether defendants acquired UserWeb documents containing trade secrets through improper means, namely misappropriation.

Second, and alternatively, misappropriation occurs under subsection (b) when a person:

> [d]isclos[es] or us[es] without express or implied consent a trade secret of another if the person did any of the following:
>
> 1. Used improper means to acquire knowledge of the trade secret.
>
> 2. At the time of disclosure or use, knew or had reason to know that he or she obtained knowledge of the trade secret through any of the following means:
>
> a. Deriving it from or through a person who utilized improper means to acquire it.
>
> b. Acquiring it under circumstances giving rise to a duty to maintain its secrecy or limit its use.

> c. Deriving it from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use.
>
> d. Acquiring it by accident or mistake.

Wis. Stat. § 134.90(2).

Critically, this prong of the UTSA requires evidence of disclosure or use as a threshold element. In the discussion of plaintiff's breach of contract claim above, the court noted that the evidence of improper use -- namely, Epic's evidence of TCS using documents from the UserWeb to further its development of Med Mantra and related software products -- was not so one-sided as to warrant judgment in plaintiff's favor on certain of its breach of contract theories. Now presented with *defendants'* motion for summary judgment on a claim premised on improper use, the court must consider whether plaintiff's evidence is sufficient for a reasonable jury to find in its favor.

If plaintiff were solely relying on the fact that TCS admits its employees did not need to access the UserWeb to perform their work for Kaiser, the court may well agree with defendants that this evidence is not sufficient for the jury to find improper use. As detailed above in the court's discussion of plaintiff's breach of contract claim (*see supra* Opinion § I.A), however, plaintiff presents other evidence in support of its claim. Namely, plaintiff points to (1) the comparative analysis conducted in 2014, where members of the Kaiser team were involved in providing information about Epic's software, and an earlier attempt to develop such an analysis for purposes of competing with Epic in selling software to Kaiser; (2) the downloading of documents relating to Epic's Beaker (laboratory) module, which Kaiser did not use; and (3) TCS's development

of a laboratory software product for a Colorado hospital around the same period of time. The court finds that this evidence provides a sufficient basis from which a reasonable jury could (though certainly need not) infer improper use.[44]

C. Conversion

Finally, defendants seek summary judgment on plaintiff's conversion claim under Wisconsin common law, arguing that a conversion claim is limited to tangible property or chattel and does not cover intellectual property, like that at issue here. In the opinion on defendants' motion to dismiss, the court denied defendants' motion to dismiss plaintiff's conversion claim, in part because "courts from other jurisdiction have recognized that electronic documents are the proper subject of conversion claims." (11/18/15 Op. & Order (dkt. #243) 16 n.7.) At summary judgment, defendants offer additional support for its argument that this claim should fail as a matter of Wisconsin law. In particular, TCS directs the court to district court cases, including one from this district, holding that a common law action for conversion under Wisconsin law is limited to tangible property. *See Rigsby v. Am. Family Mut. Ins. Co.*, No. 14-cv-23-bbc, 2014 WL 1515493, at *7 (W.D. Wis. Apr. 17, 2014); *Maryland Staffing Servs., Inc. v. Manpower, Inc.*, 936 F. Supp. 1494, 1507 (E.D. Wis. 1996).

As the court previously noted and plaintiff again points out, however, other courts have recognized "the contemporary realities of widespread computer use" and have

[44] Barring directions to the jury, of course, either side may want to present evidence of plaintiff's efforts to locate direct evidence of use, and in the case of plaintiff, defendants claimed steps to thwart its investigation, or in the case of defendants, plaintiff's purported failure to find any evidence of misuse. The jury will have to decide if plaintiff's proof is sufficient to show misuse.

broadened the common law claim to include "electronic records that are stored on a computer." (Pl.'s Opp'n (dkt. #414) 43 (quoting *Thyroff v. Nationwide Mut. Ins. Co.*, 864 N.E.2d 1272, 1278 (N.Y. 2008)).) *See also Aventa Learning, Inc. v. K12 Inc.*, 830 F. Supp. 2d 1083, 1105 (W.D. Wash. 2011); *E. I. DuPont DeNemours & Co. v. Kolon Indus., Inc.*, 688 F. Supp. 2d. 443, 454-55 (E.D. Va. 2009). While the court finds the reasoning of these courts compelling, there is, at least so far, no support from Wisconsin courts for such an expansion of this state's common law -- at least, plaintiff has failed to direct the court's attention to such cases.[45]

Absent some indication that Wisconsin courts would embrace such an expansion, the court is unwilling to adopt a broader definition of a conversion claim then currently is recognized based solely on intangible property, especially where plaintiff has other applicable claims (*e.g.*, the computer fraud claims under both federal and state law described above) and the Wisconsin Supreme Court's continued narrowing of the availability of tort remedies in a commercial setting, particularly where the parties' principal relationship is defined by contract. *See generally* 3 Dan B. Dobbs, *et al.*, The Law of Torts § 712 (2d ed. 2011) ("The effect of the rule against conversion of intangibles as

[45] In a case decided under Illinois law that dates back some 25 years, the Seventh Circuit also refused to recognize a conversion claim based on the copying of electronic documents, explaining:

> The reason for this rule is that the possession of copies of documents—as opposed to the documents themselves—does not amount to an interference with the owner's property sufficient to constitute conversion. In cases where the alleged converter has only a copy of the owner's property and the owner still possesses the property itself, the owner is in no way being deprived of the use of his property. The only rub is that someone else is using it as well.

FMC Corp. v. Capital Cities/ABC, Inc., 915 F.2d 300, 303-04 (7th Cir. 1990) (internal citation omitted).

well as the cluster of economic loss rules is to channel analysis to the tort most particularly designed to deal with the facts."); John J. Laubmeier, Comments, *Demystifying Wisconsin's Economic Loss Doctrine*, 2005 Wis. L. Rev.. 225, 229 (2005) ("Since the initial recognition of the economic loss doctrine, Wisconsin courts have significantly expanded the doctrine's scope and breadth."). Accordingly, the court will grant defendants' motion for summary judgment on plaintiff's claim.

III. Epic's Rule 56(d) Motion and Remaining Discovery Disputes

In addition to the parties' motions for summary judgment, there are three other motions before the court. First, on the same day plaintiff filed its opposition to defendants' motion for summary judgment, plaintiff also filed a motion for an order denying or deferring consideration of defendant's motion for partial summary judgment under Federal Rule of Civil Procedure 56(d). (Dkt. #413.) In particular, plaintiff sought to head off any argument by defendants that it failed to come forth with sufficient evidence to support a jury's finding of improper use, directing the court to its ongoing efforts to secure certain discovery and defendants' repeated attempts to hinder those efforts. Because the court finds on the summary judgment record, that plaintiff *has* put forth sufficient evidence to support such a jury finding in its favor on improper use (*see supra* Opinion §§ I.A, II.B), the court need not consider plaintiff's motion under Rule 56(d), and therefore will deny it as moot.

Also before the court is plaintiff's motion to compel responses to its fourth set of interrogatories. (Dkt. #448.) While this discovery is not necessary to oppose TCS's motion for summary judgment for the reasons already explained, a question obviously

remains as to whether responses to plaintiff's remaining requests would further its ability to prove its claims at trial. In its motion and supporting brief, plaintiff seeks three categories of information. *First*, plaintiff seeks responses to interrogatories requesting the source of information relied on in TCS's comparative analysis of Epic to Med Mantra. Specifically, in light of defendants' representation that the comparative analysis was compiled (or at least *could* have been compiled) from publicly available information about Epic, plaintiff reasonably seeks the source of that public information.

In response, defendants contend that the main compiler of the comparative analysis, Naresh Yallapragada, is no longer an employee, and therefore, defendants cannot produce him for a deposition and he has not responded to their requests to appear voluntarily. (Defs.' Opp'n (dkt. #464) 4.) Moreover, defendants contend that "TCS's knowledge of the source of the information used in the comparative analysis comes from deposition testimony and documents produced by TCS, all of which is equally known to Epic." (*Id.* at 5.)

Perhaps defendants have exhausted all reasonable efforts to respond to this interrogatory. After all, it was certainly in *defendants'* interest to direct plaintiff to specific portions of deposition excerpts or documents produced in this case that demonstrate (or, at least, support) TCS's assertion that the comparative analysis was prepared with public information, as well as to other publicly available information that *may* have been used. Regardless, the court is not inclined to require defendants to respond further. Instead, defendants will be *barred* from further supplementing their responses, and plaintiff may point out defendants' failure to come forward with specific examples in support of its

theory that Yallapragada or others relied or could have relied on publicly-available information to develop his comparative analysis, unless previously, specifically designated or disclosed in answer to these interrogatories.

Second, Epic seeks an order compelling TCS to reveal the identity of the person referenced in a May 2012 email, which states in relevant part: "There was one guy in our team who had access to EPIC. He left us recently. Now, we have no one. Dire state." (Pl.'s Br. (dkt. #449) 8.) In depositions, Epic has asked several individuals involved in the email to identify the "one guy," but no one could provide the identity. (*Id.* at 8-9.) In its response to plaintiff's motion, defendants indicate that they have since learned the identity of the person was Dambaraudhara Behera. Accordingly, the court will deny this second request as moot.

Third, Epic seeks to compel a response to an interrogatory asking TCS to identify by bates number emails sent from the @tcs.com email address to a @kp.org email in order to match each email with the documents downloaded from an Indian IP address. After further clarification from Epic, defendants contend in their response that they have now provided a list of the documents in a supplemental response. Accordingly, the court will deny this request as moot as well.

Finally, the court must consider defendants' own recently-filed motion to compel responses to its third set of interrogatories. (Dkt. #484.) In its brief in support, defendants represent that plaintiff's recent forensic investigation "did not turn up any evidence of the downloaded documents on TCS's system." Accordingly, defendants seek an order compelling plaintiff to answer four interrogatories confirming this lack of

evidence. (Defs.' Br. (dkt. #485) 2, 7.) The court (particularly Judge Crocker) has had to devote far too much time and resources sorting through the parties' numerous discovery disputes to spend *any* time on a motion cast as a discovery dispute, but which is really just a thinly-veiled attempt at a sur-reply in support of defendants' motion for summary judgment. The motion is improper, and the court will deny it without further consideration.[46]

[46] As previously noted, barring further direction from the court, defendants remain free to offer evidence of investigative efforts by both sides and the results of those investigations at trial, just as plaintiff may offer evidence and posit reasons why this is so.

ORDER

IT IS ORDERED that:

1) Plaintiff Epic System Corporation's motion for partial summary judgment (dkt. #195) is GRANTED IN PART AND DENIED IN PART. The motion is granted as to (a) breach of contract claims based on (i) failure to provide written notice of unauthorized use and (ii) failure to maintain confidential information in confidence and secure documents in a secure placed based on a TCS's employee's emailing of an Epic document to an individual not employed by TCS; (b) the first element of the Computer Fraud and Abuse Act, 19 U.S.C. §1030(g), finding a violation of the CFAA based on defendants' unauthorized access; and (c) Wisconsin Computer Crimes Act, Wis. Stat. § 943.70(2)(a), claim based on unauthorized access and sharing of password information. In all other respects, the motion is denied.

2) Defendants Tata America International Corporation and Tata Consultancy Services Limited's motion for partial summary judgment (dkt. #197) is GRANTED IN PART AND DENIED IN PART. Defendants' motion for summary judgment as to plaintiff's conversion claim is granted. In all other respects, the motion is denied.

3) Plaintiff's motion for an order denying or deferring consideration of defendants' partial motion for summary judgment (dkt. #413) is DENIED.

4) Plaintiff's motion to compel responses to its fourth set of interrogatories (dkt. #448) is GRANTED IN PART as to defendants being bound by to its current, non-specific response to plaintiff's interrogatories regarding alternative sources of information available to prepare TCS's comparative analysis of EPIC and Med Mantra products and DENIED IN PART AS MOOT as described above.

5) Defendants' motion to compel responses to defendants' third set of interrogatories (dkt. #484) is DENIED.

6) Plaintiff's expedited motion to dismiss defendants' counterclaims and to immediately sever and stay all counterclaim proceedings (dkt. #326) is GRANTED IN PART AND RESERVED IN PART. The counterclaims are severed and all proceedings on the counterclaims are stayed until the court issues its decision on plaintiff's motion to dismiss.

Entered this 27th day of July, 2016.

BY THE COURT:
/s/
WILLIAM M. CONLEY
District Judge